

PowerProtect Data Manager 19.9

Administration and User Guide

Version 19.9

Notes, cautions, and warnings

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

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

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

Preface.....	11
Chapter 1: Getting Started.....	15
Introducing the PowerProtect Data Manager software.....	15
Supported Internet Protocol versions.....	16
References.....	16
Terminology.....	17
Access the PowerProtect Data Manager UI.....	18
Getting Started window.....	18
UI tools and options	19
Provide customer feedback.....	21
Role-based security.....	22
Chapter 2: Managing Users.....	23
Managing identity providers.....	23
Configure an external identity provider.....	23
Edit an external identity provider.....	24
Delete an external identity provider.....	25
Managing user roles and privileges	25
Managing local identity provider users.....	25
Add a local user.....	25
Edit or delete a local user.....	26
Common password policy.....	26
Change a local user password.....	27
Reset a forgotten local user password.....	27
Reset operating system passwords.....	27
Default authorizations.....	28
System-provided roles and associated privileges.....	28
Role privilege definitions.....	31
External authorization associations.....	34
Add identity provider group-to-role mapping.....	34
Modify identity provider group-to-role mapping.....	34
Delete identity provider group-to-role mapping.....	35
Remote component authentication.....	35
Add a credential.....	35
View credential usage.....	36
Edit a credential.....	36
Delete credentials.....	36
Credential security.....	37
Chapter 3: Managing Storage.....	38
Protection storage.....	38
High Availability PowerProtect DD support.....	38
Add protection storage.....	39
Edit protection storage.....	40

Storage units.....	40
Storage unit limitations.....	41
Storage unit considerations for PowerProtect DD.....	41
Create a storage unit.....	42
Edit a storage unit.....	43
Change a storage unit password.....	44
View the storage unit password.....	45
Overview of PowerProtect Data Manager Cloud Tier.....	45
Chapter 4: Using the PowerProtect Search Engine.....	46
Introducing the PowerProtect Search Engine.....	46
Set up and manage indexing.....	46
Search Engine node deletion.....	48
Delete operational nodes from a Search cluster.....	48
Redeploy or delete failed nodes from a Search cluster.....	49
Edit the network configuration for a search engine node.....	49
Perform a search.....	50
Virtual machine file level restore from a search.....	50
File level restore to original virtual machine using File Search.....	50
File level restore to alternate virtual machine using File Search.....	51
Troubleshooting Search Engine issues.....	52
Chapter 5: Managing Assets.....	58
About asset sources, assets, and storage.....	58
About vCenter Server asset sources and virtual assets.....	58
About other asset sources.....	58
Prerequisites for discovering asset sources.....	59
Enable an asset source.....	60
Disable an asset source.....	61
Delete an asset source.....	61
Adding a vCenter Server asset source.....	61
Add a VMware vCenter Server.....	62
Creating a dedicated vCenter user account.....	63
VM Direct protection engine overview.....	66
Requirements for an external VM Direct Engine.....	66
Add a VM Direct Engine.....	66
Additional VM Direct actions.....	68
Transparent Snapshot Data Mover protection mechanism.....	70
Adding a Cloud Snapshot Manager tenant.....	72
Add a Cloud Snapshot Manager Tenant.....	72
Chapter 6: Managing Protection Policies.....	73
Protection policies.....	73
Before you create a protection policy.....	74
Supported enhanced VMware topologies for virtual-machine protection.....	76
Add a protection policy for virtual-machine protection.....	77
Managing virtual-machine backups.....	84
Add a Cloud Tier schedule to a protection policy.....	86
Manage Cloud Tier asset copies.....	87

Manual backups of protected assets.....	88
Manual replication of protected assets.....	88
Manual Cloud Tiering of protected assets.....	89
Editing a protection policy.....	89
Modify a policy name and description, objectives, or options.....	89
Changing storage targets and storage units.....	90
Add or remove assets in a protection policy.....	91
View assets assigned to a protection policy.....	92
Extended retention.....	93
Edit the retention period for backup copies.....	94
Delete backup copies.....	95
Retry a failed backup copy deletion.....	96
Export data for deleted backup copies.....	96
Remove backup copies from the PowerProtect Data Manager database.....	97
Removing expired backup copies.....	97
Removing assets from PowerProtect Data Manager.....	98
Remove assets and associated protection copies.....	98
Export protection	99
Disable a protection policy.....	99
Protection jobs running for a disabled policy.....	100
Enable a disabled protection policy.....	101
Customize the default behavior of disabled policies.....	101
Delete a protection policy.....	101
Add a Service Level Agreement.....	102
Export Asset Compliance.....	104
Protection rules	105
Creating virtual machine tags in the vSphere Client.....	105
Add a protection rule.....	106
Manually run a protection rule.....	107
Edit or delete a protection rule	108
View assets applied to a protection rule.....	108
Change the priority of an existing protection rule	108
Configure protection rule behavior.....	109
Chapter 7: Restoring Data and Assets.....	110
View backup copies available for restore.....	110
Restoring a virtual machine or VMDK.....	111
Restoring a virtual machine backup with the storage policy association.....	111
Prerequisites to restore a virtual machine.....	112
Restore to the original virtual machine.....	112
Restore individual virtual disks.....	114
Restore to a new virtual machine.....	115
Instant access virtual machine restore.....	117
File level restore to original virtual machine.....	120
File level restore to alternate virtual machine.....	121
Direct restore to ESXi.....	122
Restore an application-aware virtual machine backup.....	123
Restore the PowerProtect Data Manager server	123
Restore Cloud Tier backups to protection storage.....	124
Recall and restore from Cloud Tier.....	124

Chapter 8: Preparing for and Recovering From a Disaster.....	126
Managing system backups for server disaster recovery.....	126
Server DR protection storage types.....	126
Overview of PowerProtect Data Manager Cloud Disaster Recovery.....	127
Prepare the DD system recovery target (NFS).....	127
Configure PowerProtect Data Manager server DR backups.....	128
Record settings for server DR.....	129
Manage PowerProtect Data Manager server DR backups.....	129
Restore PowerProtect Data Manager from server DR backups.....	130
Recovering the Search Engine from a DR backup.....	131
Troubleshooting NFS backup configuration issues.....	132
Troubleshoot recovery of PowerProtect Data Manager.....	133
Quick recovery.....	133
Quick recovery prerequisites.....	136
Add a remote system for quick recovery.....	137
Edit a remote system.....	137
Quick recovery remote view.....	138
Recover a failed PowerProtect Data Manager backup.....	138
 Chapter 9: Managing Alerts, Jobs, and Tasks.....	 139
Configure Alert Notifications.....	139
View and manage alerts.....	139
View and manage Audit Logs.....	140
Monitoring jobs and tasks.....	140
Monitor and view jobs.....	141
View details for protection jobs.....	142
View details for system jobs and tasks.....	144
Filter, group, and sort jobs.....	146
Restart a job or task manually.....	148
Restart a job or task automatically.....	148
Resume misfire jobs after a PowerProtect Data Manager update.....	149
Cancel a job or task.....	150
Exporting logs.....	151
Export logs for jobs.....	152
Export logs for assets or tasks.....	152
 Chapter 10: Modifying the System Settings.....	 153
System settings.....	153
Modify the network settings.....	153
Synchronize time on PowerProtect Data Manager and other systems.....	153
Modify the appliance time zone.....	154
Enable replication encryption.....	154
Backup and restore encryption.....	154
PowerProtect Data Manager licensing.....	156
Specify a vCenter Server as the PowerProtect Data Manager host.....	157
System Support.....	158
Configuring SupportAssist for PowerProtect Data Manager.....	158
Telemetry Collector	162

CloudIQ reporting.....	163
Set up the email server.....	163
Add AutoSupport.....	163
Enabling automatic update package checks and downloads.....	164
Add a log bundle.....	164
Audit logging and monitoring system activity.....	164
Monitor system state and system health.....	166
Access the open source software package information.....	166
Security certificates.....	166
Modifying the PowerProtect Data Manager virtual machine disk settings.....	167
Modify the data disk size.....	167
Modify the system disk size.....	168
Memory optimization.....	168
Adjust the memory.....	169
Configure the DD system.....	169
Virtual networks (VLANs).....	170
Supported scenarios.....	171
Virtual network prerequisites.....	171
Configuring virtual networks.....	172
Virtual network asset assignment.....	174
Chapter 11: Protecting Virtual Machines using the Transparent Snapshot Data Mover	177
Overview of transparent snapshots for virtual machine protection.....	177
VIB installation monitoring and management.....	177
Transparent snapshot data mover system requirements.....	178
Prerequisites to virtual machine protection with the Transparent Snapshot Data Mover.....	178
Additional privileges required for a dedicated vCenter user account to use Transparent Snapshot Data Mover.....	178
Creating VMkernel ports.....	179
Virtual machine transparent snapshot unsupported features and limitations.....	180
Transparent Snapshot Performance and Scalability.....	181
Chapter 12: PowerProtect Functionality Within the vSphere Client.....	182
PowerProtect functionality within the vSphere Client.....	182
Overview of the PowerProtect plug-in for the vSphere Client.....	182
Prerequisites for enabling the vSphere Client PowerProtect plug-in.....	183
Monitor PowerProtect Data Manager virtual machine protection copies.....	184
Manual PowerProtect policy backup in the vSphere Client.....	185
Image-level restore of a PowerProtect backup in the vSphere Client.....	185
File-level restore of a PowerProtect backup in the vSphere Client.....	186
Overview of VASA and VMware Storage Policy Based Management	188
Register the VASA provider for policy association.....	188
Add an SPBM policy and associate with a PowerProtect Data Manager virtual machine policy.....	189
Monitor virtual machine protection policy compliance.....	190
Chapter 13: VMware Cloud (VMC) on Amazon Web Services (AWS).....	191
PowerProtect Data Manager image backup and recovery.....	191
Supported PowerProtect Data Manager and DDVE deployment configurations.....	191
Deployment and configuration best practices and requirements.....	192

Configuring the VMC-on-AWS portal.....	192
Interoperability with PowerProtect Data Manager features.....	193
vCenter server inventory requirements.....	193
Creating a dedicated cloud-based vCenter user account.....	193
Specify the required privileges for a dedicated cloud-based vCenter user account	193
Add a VM Direct Engine.....	195
Unsupported operations	197
Chapter 14: Azure VMware Solution (AVS) on Microsoft Azure.....	198
PowerProtect Data Manager image backup and recovery.....	198
Supported PowerProtect Data Manager and DDVE deployment configurations.....	198
Deployment and configuration best practices and requirements.....	199
Configuring the AVS-on-Azure portal.....	199
vCenter server inventory requirements.....	200
Creating a dedicated cloud-based vCenter user account.....	200
Specify the required privileges for a dedicated cloud-based vCenter user account	200
Add a VM Direct Engine.....	202
Unsupported operations	203
Chapter 15: Google Cloud VMware Engine (GCVE) on Google Cloud Product (GCP).....	204
PowerProtect Data Manager image backup and recovery.....	204
Supported PowerProtect Data Manager and DDVE deployment configurations.....	204
Deployment and configuration best practices and requirements.....	205
Configuring the GCVE-on-GCP portal.....	205
vCenter server inventory requirements.....	206
Creating a dedicated cloud-based vCenter user account.....	206
Specify the required privileges for a dedicated cloud-based vCenter user account	206
Add a VM Direct Engine.....	208
Unsupported operations.....	209
Chapter 16: Performing Updates.....	210
Managing update packages.....	210
Automatically check for an update package.....	210
Troubleshooting automatic downloads.....	211
Manually check for an update package.....	211
Download an update package.....	211
Upload an update package.....	212
Delete an update package.....	212
Perform a precheck on an update package.....	212
Install an update package.....	213
Updating the version of PowerProtect Data Manager.....	213
Update PowerProtect Data Manager from version 19.8 to version 19.9.....	214
Update PowerProtect Data Manager from version 19.7 to version 19.9.....	216
Update PowerProtect Data Manager from versions 19.3–19.6 to version 19.9.....	218
Run a manual precheck.....	221
Lockbox passphrase required when updating from some versions.....	221
Chapter 17: Configuring and Managing the PowerProtect Agent Service	223
About the PowerProtect agent service.....	223

Start, stop, or obtain the status of the PowerProtect agent service.....	224
Register the PowerProtect agent service to a different server address.....	224
Recovering the PowerProtect agent service from a disaster.....	225
Restore the PowerProtect Data Manager agent service datastore.....	225
Chapter 18: Backing Up and Recovering a vCenter Server.....	227
Backing up and recovering a vCenter server.....	227
vCenter deployments overview.....	227
Protecting an embedded PSC.....	227
Direct restore to ESXi.....	228
Protecting external deployment models.....	229
vCenter server appliance(s) with one external PSC where PSC fails.....	229
vCenter server appliance is lost but the PSC remains.....	230
vCenter server appliance with multiple PSCs where one PSC is lost, one remains.....	230
vCenter server appliance remains but all PSCs fail.....	230
vCenter server appliance remains but multiple PSCs fail.....	230
vCenter server appliance fails.....	231
vCenter server restore workflow.....	232
Platform Services Controller restore workflow.....	233
Additional considerations.....	233
Command reference.....	234
Chapter 19: Backing Up VMware Cloud Foundation (VCF) on VxRail.....	235
Backing up VCF on VxRail.....	235
VCF and VxRail overview.....	235
VCF components and backup methods.....	236
Check VMware certification.....	237
Backup prerequisites.....	237
The backup script.....	237
Quick protection.....	237
Selective protection: SDDC and NSX-T Managers.....	239
Selective protection: vCenter servers.....	240
Selective protection: vRSLCM, VxRail Manager, Workspace ONE Access, and vRealize Suite virtual machines.....	241
SFTP password change: SDDC and NSX-T Managers.....	241
SFTP password change: vCenter servers.....	242
Backup-script troubleshooting.....	243
Chapter 20: Best Practices and Troubleshooting.....	245
Base 10 standard used for size calculations in the PowerProtect Data Manager UI.....	245
Best practices and additional considerations for the VM Direct Engine.....	245
Change the limit of instant access sessions.....	245
Configuring a backup to support vSAN datastores.....	246
Configuration checklist for common issues.....	246
Disable vCenter SSL certificate validation.....	246
File-level restore and SQL restore limitations.....	247
FLR Agent for virtual machine file level restore.....	248
FLR-supported platform and OS versions for virtual machine restores.....	250
PowerProtect Data Manager resource requirements in a VMware environment.....	251

Software and hardware requirements.....	251
Support for backup and restore of encrypted virtual machines.....	252
Transport mode considerations.....	252
Virtual disk types supported.....	253
Virtual machine data change rate.....	253
VM Direct Engine data ingestion rate.....	254
VM Direct Engine limitations and unsupported features.....	254
VM Direct Engine performance and scalability.....	257
VM Direct Engine selection with virtual networks (VLANs).....	258
Best practices for vCenter Server backup and restore.....	258
Changing the vCenter server FQDN.....	258
Change the vCenter server FQDN.....	258
Monitoring storage capacity thresholds.....	259
Replacing security certificates.....	260
Replacing the self-signed security certificates.....	260
Replace expired or changed certificates on an external server.....	260
Restarting PowerProtect Data Manager.....	262
Scalability limits for vCenter Server, VM Direct Engine and DD systems.....	262
Troubleshooting network setup issues.....	263
Troubleshooting PowerProtect agent service installations.....	263
Troubleshooting PowerProtect agent service operations.....	263
Troubleshoot the PowerProtect agent service operations.....	263
Troubleshooting PowerProtect Data Manager software updates.....	264
Managing certificates after updating PowerProtect Data Manager from versions earlier than 19.1... ..	264
Troubleshooting storage units.....	265
Troubleshooting virtual machine backup issues.....	265
Backup completes with a non-quiesced snapshot warning.....	265
Backup fails when names include special characters	266
Deleting vCenter asset sources or moving ESXi to another vCenter.....	266
Failed to lock Virtual Machine for backup: Another EMC vProxy operation 'Backup' is active on VM	267
Lock placed on virtual machine during backup and recovery operations continues for 24 hours if VM Direct appliance fails.....	267
Managing command execution for VM Proxy Agent operations on Linux.....	268
PowerProtect plug-in and portlet for vSphere display errors after replacing security certificates.....	268
SQL databases skipped during virtual machine transaction log backup.....	268
SQL Server application-aware backup displays an error about disk.EnableUUID variable.....	269
SQL Server application-consistent backups fail with error "Unable to find VSS metadata files in directory".....	269
Trailing spaces not supported in SQL database names.....	269
VMware knowledge base articles and product documentation.....	269
Troubleshooting virtual machine restore issues.....	269
Troubleshooting instant access restore failures.....	271
VMware knowledge base articles and product documentation.....	272
Troubleshooting vSphere Plugin deployments.....	272
Troubleshoot vSphere Plugin deployments.....	272
VMware knowledge base articles and product documentation.....	272

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 Customer Support.

NOTE: This document was accurate at publication time. To ensure that you are using the latest version of this document, go to the [Customer Support](#) website.

Data Domain (DD) is now PowerProtect DD. References to Data Domain or Data Domain systems in this documentation, in the user interface, and elsewhere in the product include PowerProtect DD systems and older Data Domain systems. In many cases the user interface has not yet been updated to reflect this change.

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

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

Purpose

This document describes how to configure and administer Dell EMC 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 Dell EMC PowerProtect Data Manager software.

Revision history

The following table presents the revision history of this document.

Table 1. Revision history

Revision	Date	Description
02	January, 2022	Updated memory requirements and guidance.
01	September, 2021	Initial release of this document for PowerProtect Data Manager version 19.9.

Compatibility information

Software compatibility information for the PowerProtect Data Manager software is provided at the [eLab Navigator](#).

Related documentation

The following publications are available at [Customer Support](#) and provide additional information:

- *PowerProtect Data Manager Administration and User Guide*—Describes how to configure the software.
- *PowerProtect Data Manager Deployment Guide*—Describes how to deploy the software.
- *PowerProtect Data Manager Licensing Guide*—Describes how to license 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 AWS Deployment Guide*—Describes how to deploy the software to Amazon Web Services (AWS).
- *PowerProtect Data Manager Azure Deployment Guide*—Describes how to deploy the software to Microsoft Azure.
- *PowerProtect Data Manager GCP Deployment Guide*—Describes how to deploy the software to Google Cloud Platform (GCP).
- *PowerProtect Data Manager Cloud Disaster Recovery Administration and User Guide*—Describes how to deploy Cloud DR, protect VMs in the AWS or Azure cloud, and run recovery operations.
- *PowerProtect Data Manager for Cyber Recovery User Guide*—Describes how to install, update, patch, and uninstall the Dell EMC PowerProtect Cyber Recovery software.
- *PowerProtect Data Manager for File System Agent User Guide*—Describes how to configure and use the software with the File System agent for file system data protection.
- *PowerProtect Data Manager for Kubernetes User Guide*—Describes how to configure and use the software to protect and recover namespaces and PVCs in a Kubernetes cluster.
- *PowerProtect Data Manager for Microsoft Application Agent Exchange Server User Guide*—Describes how to configure and use the software to protect and recover the data in a Microsoft Exchange Server environment.
- *PowerProtect Data Manager for Microsoft Application Agent SQL Server User Guide*—Describes how to configure and use the software to protect and recover the data in a Microsoft SQL Server environment.
- *PowerProtect Data Manager for Oracle RMAN Agent User Guide*—Describes how to configure and use the software to protect and recover the data in an Oracle Server environment.
- *PowerProtect Data Manager for SAP HANA Agent User Guide*—Describes how to configure and use the software to protect and recover the data in an SAP HANA Server environment.
- *PowerProtect Data Manager for Storage Direct Agent User Guide*—Describes how to configure and use the software with the Storage Direct agent to protect data on VMAX storage arrays through snapshot backup technology.
- *PowerProtect Data Manager for Network Attached Storage User Guide*—Describes how to configure and use the software to protect and recover the data on network attached storage (NAS) shares and appliances.
- [PowerProtect Data Manager Public REST API documentation](#)—Contains the PowerProtect Data Manager APIs and includes tutorials to guide you in their use.

Typographical conventions

The following type style conventions are used in this document:

Table 2. Style conventions

Formatting	Description
Bold	Used for interface elements that a user specifically selects or clicks, for example, names of buttons, fields, tab names, and menu paths. Also used for the name of a dialog box, page, pane, screen area with title, table label, and window.
<i>Italic</i>	Used for full titles of publications that are referenced in text.
Monospace	Used for: <ul style="list-style-type: none"> • System code • System output, such as an error message or script • Pathnames, file names, file name extensions, prompts, and syntax • Commands and options
<i>Monospace italic</i>	Used for variables.
Monospace bold	Used for user input.
[]	Square brackets enclose optional values.
	Vertical line indicates alternate selections. The vertical line means or for the alternate selections.
{ }	Braces enclose content that the user must specify, such as x, y, or z.
...	Ellipses indicate non-essential information that is omitted from the example.

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

Where to find product documentation

- The [Customer Support](#) website
- The [Community Network](#)

Where to get support

The [Customer Support](#) website 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 Customer Support.

To access a product-specific page:

1. Go to the [Customer Support](#) website.
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 the [Customer Support](#) website.
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 the [Customer Support](#) website.
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 a support agent, submit a service request. To submit a service request:

1. Go to the [Customer Support](#) website.
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 the [Customer Support](#) website.
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](#). 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.

Getting Started

Topics:

- [Introducing the PowerProtect Data Manager software](#)
- [Supported Internet Protocol versions](#)
- [References](#)
- [Terminology](#)
- [Access the PowerProtect Data Manager UI](#)
- [Provide customer feedback](#)
- [Role-based security](#)

Introducing the 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 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
- Multicloud optimization with integrated Cloud Tiering
- SaaS-based monitoring and reporting
- Modern services-based architecture for ease of deployment, scaling, and updating

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:

- Enables the data protection team to create data paths with provisioning, automation, and scheduling to embed protection engines into the infrastructure for high-performance backup and recovery.
- Enables backup administrators of large-scale environments to schedule backups for the following asset types from a central location on the PowerProtect Data Manager server:
 - VMware virtual machines
 - File systems
 - VMAX storage groups
 - Kubernetes clusters
 - Microsoft Exchange and SQL databases
 - Oracle databases
 - SAP HANA databases
 - Network attached storage (NAS) shares
- Uses an agent-based approach to discover the protected and unprotected databases on an application server.
- Enables governed self-service and centralized protection by:
 - Monitoring Service Level Objectives (SLOs)
 - Identifying violations of Recovery Point Objectives (RPOs)
- Supports deploying an external VM Direct appliance to move data with a VM Direct Engine. The PowerProtect Data Manager software comes pre-bundled with an embedded VM Direct Engine, which is automatically used as a fallback proxy for performing backup and restore operations when the external VM Direct Engines fail or are disabled. Dell EMC recommends that you deploy external VM Direct Engines, because the embedded VM Direct Engine has limited capacity for performing backup streams. The embedded VM Direct Engine is sufficient, however, for virtual machine crash-consistent protection policies that use the Transparent Snapshot Data Mover (TSDM) protection mechanism.
- Supports the vRealize Automation DP extension, which enables provisioning of virtual machines with PowerProtect Data Manager protection, on-demand backup, and restore to the original or a new location. The *vRealize Automation Data Protection Extension for PowerProtect Data Manager Installation and Administration Guide* provides more information.
- Supports integration of Dell EMC Cloud Disaster Recovery (Cloud DR), including workflows for Cloud DR deployment, protection, and recovery operations in the AWS or Azure cloud.

- Supports PowerProtect Search, which enables backup administrators to quickly search for and restore VM file copies. The Search Service can be enabled by adding a search node to the configurable Search Engine that is autodeployed during the PowerProtect Data Manager deployment.
- Provides a RESTful interface that allows the user to monitor, configure, and orchestrate PowerProtect Data Manager. Customers can use the APIs to integrate their own automation framework or quickly write new scripts with the help of easy-to-follow tutorials.
- Integrates with Dell EMC PowerProtect Cloud Snapshot Manager to view PowerProtect Cloud Snapshot Manager jobs, alerts, and reports from a consolidated PowerProtect Data Manager dashboard.

Supported Internet Protocol versions

PowerProtect Data Manager only supports the use of IPv4 addresses.

Using an IPv6 address can result in errors or other unexpected behavior. When configuring devices to connect over the network with PowerProtect Data Manager, use only IPv4 addresses.

References

Some procedures in this document reference other publications for further details. Additionally, updates to documentation after initial publication are provided in the release notes.

The following publications, available on [Customer Support](#), provide additional product information:

- *PowerProtect Data Manager Administration and User Guide*—Describes how to configure the software.
- *PowerProtect Data Manager Deployment Guide*—Describes how to deploy the software.
- *PowerProtect Data Manager Licensing Guide*—Describes how to license 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 AWS Deployment Guide*—Describes how to deploy the software to Amazon Web Services (AWS).
- *PowerProtect Data Manager Azure Deployment Guide*—Describes how to deploy the software to Microsoft Azure.
- *PowerProtect Data Manager GCP Deployment Guide*—Describes how to deploy the software to Google Cloud Platform (GCP).
- *PowerProtect Data Manager Cloud Disaster Recovery Administration and User Guide*—Describes how to deploy Cloud DR, protect VMs in the AWS or Azure cloud, and run recovery operations.
- *PowerProtect Data Manager for Cyber Recovery User Guide*—Describes how to install, update, patch, and uninstall the Dell EMC PowerProtect Cyber Recovery software.
- *PowerProtect Data Manager for File System Agent User Guide*—Describes how to configure and use the software with the File System agent for file system data protection.
- *PowerProtect Data Manager for Kubernetes User Guide*—Describes how to configure and use the software to protect and recover namespaces and PVCs in a Kubernetes cluster.
- *PowerProtect Data Manager for Microsoft Application Agent Exchange Server User Guide*—Describes how to configure and use the software to protect and recover the data in a Microsoft Exchange Server environment.
- *PowerProtect Data Manager for Microsoft Application Agent SQL Server User Guide*—Describes how to configure and use the software to protect and recover the data in a Microsoft SQL Server environment.
- *PowerProtect Data Manager for Oracle RMAN Agent User Guide*—Describes how to configure and use the software to protect and recover the data in an Oracle Server environment.
- *PowerProtect Data Manager for SAP HANA Agent User Guide*—Describes how to configure and use the software to protect and recover the data in an SAP HANA Server environment.
- *PowerProtect Data Manager for Storage Direct Agent User Guide*—Describes how to configure and use the software with the Storage Direct agent to protect data on VMAX storage arrays through snapshot backup technology.
- *PowerProtect Data Manager for Network Attached Storage User Guide*—Describes how to configure and use the software to protect and recover the data on network attached storage (NAS) shares and appliances.
- [PowerProtect Data Manager Public REST API documentation](#)—Contains the PowerProtect Data Manager APIs and includes tutorials to guide you in their use.

Terminology

Familiarize yourself with the terminology for the PowerProtect Data Manager user interface and documentation.

The following table provides more information about names and terms that you should know to use PowerProtect Data Manager:

Table 3. Term list

Term	Description
Application Agent	Application Agents are installed on application or database host servers to manage protection using PowerProtect Data Manager. These Agents are commonly known as DD Boost Enterprise Agents (DDBEA) for databases and applications.
Application Aware	Virtual machine protection policy that includes additional application-aware data protection for Microsoft SQL Servers. An application-aware virtual machine protection policy provides the ability to quiesce the application during virtual machine image backup to perform a full backup of SQL databases. You can also schedule SQL server log backups for the virtual machines in the policy.
Asset	Assets are objects in PowerProtect Data Manager for which you want to manage protection, including VMs, databases, and file systems.
Asset Source	Assets that PowerProtect Data Manager protects reside within Asset Sources, which include vCenter Servers, application or database hosts, and file servers.
Cloud Tier Storage	Cloud Tier storage can be added to a protection storage system to expand the deduplication storage capacity onto less expensive object storage in public or private object storage clouds, including Dell EMC secure Elastic Cloud Storage appliances.
Copy	A PowerProtect Data Manager copy is a point-in-time backup copy of an Asset.
Copy Map	The PowerProtect Data Manager Copy Map is a visual representation of backup copy locations on your Protection Storage and is available for all protected Assets that have copies.
Discovery	Discovery is an internal process that scans Asset Sources to find new assets to protect and scans infrastructure components to monitor their health and status.
Instant Access	PowerProtect Data Manager VM backup copies can be accessed, mounted, and booted directly from the Protection Storage targets as running VMs. Copies can also be moved to a production VMware datastore using vMotion. PowerProtect Data Manager VM application-aware backup copies can be mounted directly from the Protection Storage targets as running SQL databases, which includes the ability to roll forward log backups. These SQL database disks can also be moved to a production VMware datastore using vMotion.
PowerProtect Data Manager Agent	An agent that is included in PowerProtect Data Manager, and installed on each application agent host server so that you can monitor and manage the application agent through PowerProtect Data Manager.
Protection Policy	Protection Policies configure and manage the entire life cycle of backup data, which includes backup type, assets, backup start/stop time, backup device, and backup retention.
Service Level Agreement (SLA)	An optional policy that you can layer on top of a Protection Policy. An SLA performs additional checks on protection activities to ensure that protection goals meet the standards that your organization requires. SLAs are made up of one or more Service Level Objectives.
Service Level Objectives (SLOs)	Definable rules that set the criteria for Recovery Point Objectives (RPOs), encryption, and locations of backups according to your company requirements.

Access the PowerProtect Data Manager UI

PowerProtect Data Manager provides a web-based UI that you can use to manage and monitor system features and settings from any location over a network.

Steps

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 username and password.

Username format: **user[@domain]**, where **domain** is an optional identifier that associates the user with a particular identity provider.

For example: **jsmith** or **administrator@test-lab**.

- If you do not supply a domain, the authentication service checks the default identity provider.
- If you supply a domain, the authentication service consults the external identity provider for that domain and determines whether to allow the login.

When the identity provider validates the credentials, the authentication service issues a user token. The PowerProtect Data Manager UI uses the token information to authorize activities.

Unless you have changed the system configuration, the default identity provider is the local identity provider.

The *PowerProtect Data Manager Security Configuration Guide* provides more information about the available user roles and their associated permissions. The associated roles for an account determine what parts of the UI a user can see and use, and what operations a user can perform.

If this is your first time accessing the PowerProtect Data Manager UI, an unsigned certificate warning might appear in the web browser.

The security certificate that encrypts communication between the PowerProtect Data Manager UI and the web browser is self-signed. A self-signed certificate is signed by the web server that hosts the secure web page. There is nothing wrong with this certificate. This certificate is sufficient to establish an encrypted channel between the web browser and the server. However, it is not signed by a trusted authority.

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.

Getting Started window

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

This window 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 clicking , and then selecting **Getting Started**.

Table 4. PowerProtect Data Manager Getting Started menu items

Options	Description
Support	View and configure SupportAssist, Email Setup, AutoSupport, Logs, System Health.
Disaster Recovery Backup	Configure and manage backups for disaster recovery.
VMware vCenter	Opens the Infrastructure > Asset Sources window, where you can add a vCenter instance as an asset source so that virtual machine assets can be added to a protection policy.
Protect Assets	Opens the Protection > Protection Policies window, where you can manage protection policy workflows for all asset types.

UI tools and options

Learn about the available tools in the UI.

PowerProtect Data Manager UI tools

Table 5. PowerProtect Data Manager tools









Menu item	Description
 Dashboard	<p>Provides a high-level view of the overall state the PowerProtect Data Manager system and includes the following information:</p> <ul style="list-style-type: none">• Alerts—System alerts• Protection—Details about protection policies• Jobs—Details and status of system and protection jobs. You can use the Protection Jobs and System Jobs windows to manage jobs, search, and view details. Filter and sort the information that appears to find specific jobs or tasks.• Policy—Details include number of successes, failures, and excluded assets for each asset type• Protection Storage—Protection storage usage statistics• Restore—Restore statistics• Compliance—Compliance verification statistics. By default, the in compliance asset count and out of compliance asset count displays for all asset types. You can select a specific asset type from the Asset Type list to display compliance statistics for only that category. <p>PowerProtect Data Manager refreshes the data hourly unless you run an ad hoc discovery.</p>
 Infrastructure	<p>Click Infrastructure to:</p> <ul style="list-style-type: none">• View and manage all assets:<ul style="list-style-type: none">◦ VMware virtual machines◦ File systems◦ VMAX storage Groups◦ Kubernetes clusters◦ Microsoft Exchange◦ SQL databases◦ Oracle databases◦ SAP HANA databases• Add vCenter and application and File System host asset sources.• View and manage Integrated Storage.• Add a VM Direct appliance with the VM Direct protection engine for virtual machine data protection.• Manage the vSphere Installation Bundle (VIB) for virtual machine crash-consistent data protection performed with the Transparent Snapshot Data Mover (TSDM) protection mechanism.• Manage registration of Oracle RMAN agent, Microsoft application agent, SAP HANA agent, and File System agent.• View and manage Dell EMC Cloud Disaster Recovery.• Create and manage a Search Cluster.• Add PowerProtect Cloud Snapshot Manager tenants as asset sources for jobs, alerts, and reports.
 Protection	<p>Click Protection to:</p> <ul style="list-style-type: none">• Add protection policies to back up assets.• Manage Service Level Agreements (SLAs).• Add, edit, and delete protection rules for asset inclusion in policies.
 Restore	<p>Click Restore to:</p> <ul style="list-style-type: none">• View asset copy location details and initiate a Restore operation.• Manage Instant Access Sessions.• Use the File Search feature to find and restore virtual machine file copies.









Table 5. PowerProtect Data Manager tools (continued)

Menu item	Description
 Alerts	Click Alerts to: <ul style="list-style-type: none"> • View and acknowledge alerts and events. • View and examine Audit logs. • Export audit logs to CSV files. • Set audit log boundaries.
 Administration	Click Administration to: <ul style="list-style-type: none"> • Configure users and roles. • Set password credentials and manage key chains. • View certificates. • Configure alert notifications. • Add LDAP Identity Sources.
 Jobs	Click Jobs to manage jobs, view by protection or system, filter, and view details.
 Reporting	Click Reporting to log in to CloudIQ.

Banner UI options

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


Table 6. Banner UI options

Option	Description
	Click to enter search criteria to find assets, jobs, logs, and alerts.
	Click to see recent alerts.
	Click to restore assets from replicated copies through quick recovery. This icon only appears when this system receives replicated metadata from a source system.
	Click to configure and manage PowerProtect Data Manager system network, time zone, and NTP settings, DR backups, security, licenses, updates, authentication, agent downloads, and support, and to access the Getting Started 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, access Customer Support, send feedback, or view the REST API documentation.
	Click to launch Cloud Snapshot Manager.

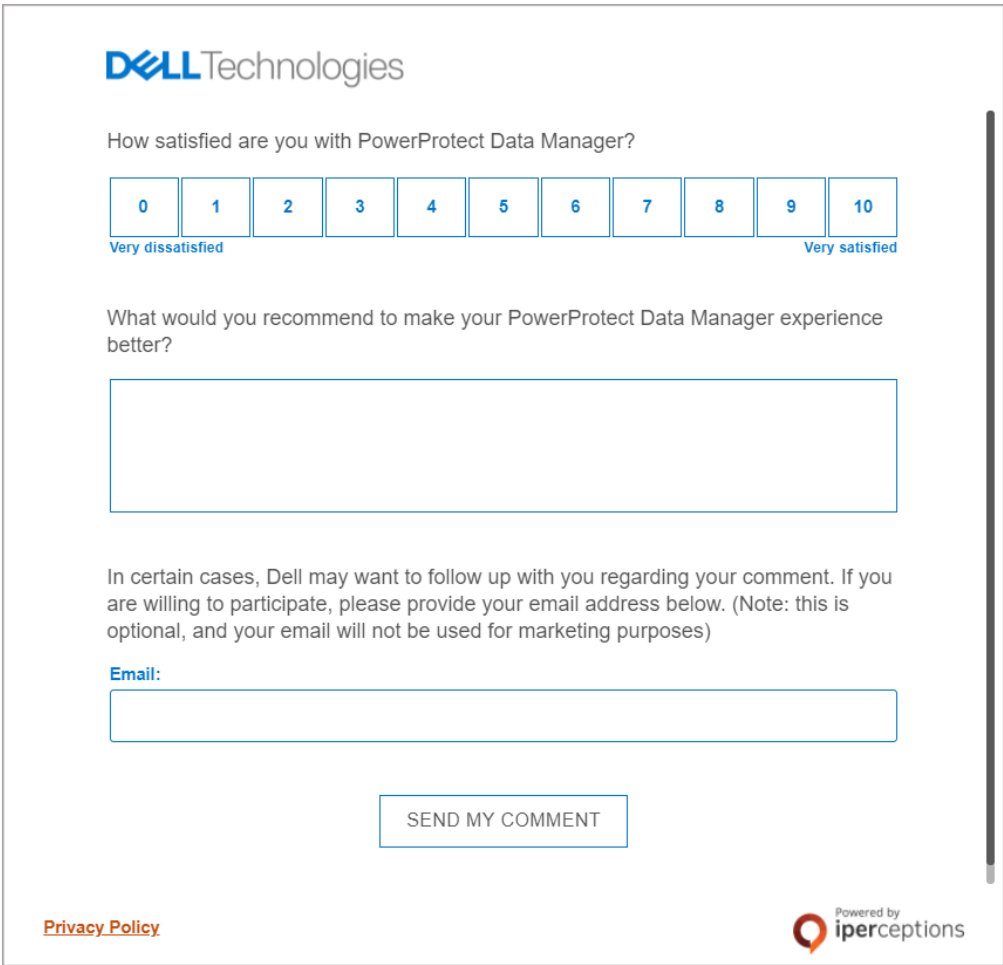
Provide customer feedback

Use the customer feedback feature in the PowerProtect Data Manager UI to report your satisfaction with PowerProtect Data Manager, provide feedback, and send requests for enhancements. Customer feedback is used to improve the customer experience with PowerProtect Data Manager.

Steps

1. Log in to the PowerProtect Data Manager UI.
2. From the banner, click , and then select **Send Feedback**.

The customer feedback survey opens in a new window, as shown in the following figure:



The screenshot shows a web form titled "Dell Technologies". The first question is "How satisfied are you with PowerProtect Data Manager?". Below it is a horizontal row of 11 buttons numbered 0 to 10. Under button 0 is the text "Very dissatisfied" and under button 10 is "Very satisfied". The second question is "What would you recommend to make your PowerProtect Data Manager experience better?". Below it is a large rectangular text input field. The third section contains the text: "In certain cases, Dell may want to follow up with you regarding your comment. If you are willing to participate, please provide your email address below. (Note: this is optional, and your email will not be used for marketing purposes)". Below this text is a label "Email:" followed by a rectangular text input field. At the bottom center is a button labeled "SEND MY COMMENT". In the bottom left corner is a link "Privacy Policy" and in the bottom right corner is the "Powered by iperceptions" logo.

Figure 1. Customer feedback survey

3. (Optional) Complete the fields in the customer feedback survey, and when finished, click **Send My Comment**.
You have the option to rate your satisfaction with PowerProtect Data Manager and make a recommendation for how to improve the customer experience. You also have the option to provide an email address so that Dell can follow up with you regarding your feedback.

 **NOTE:** Customer contact information will not be used for marketing purposes.

Role-based security

PowerProtect Data Manager provides predefined user roles that control access to areas of the user interface and to protected operations. Some of the functionality in this guide is reserved for particular roles and may not be accessible from every user account.

By using the predefined roles, you can limit access to PowerProtect Data Manager and to backup data by applying the principle of least privilege.

The *PowerProtect Data Manager Security Configuration Guide* provides more information about user roles, including the associated privileges and the tasks that each role can perform.

Managing Users

Topics:

- [Managing identity providers](#)
- [Managing user roles and privileges](#)
- [Managing local identity provider users](#)
- [Default authorizations](#)
- [System-provided roles and associated privileges](#)
- [Role privilege definitions](#)
- [External authorization associations](#)
- [Remote component authentication](#)
- [Credential security](#)

Managing identity providers

You can configure an external identity provider that manages usernames and passwords.

Only the Administrator and the Security Administrator roles can manage external identity providers. Manage identity providers and roles through the **Administration > Access Control** pane.

Configure an external identity provider

Only the Administrator and the Security Administrator roles can configure an external identity provider.

Steps

1. From the left navigation pane, select **Administration > Access Control**.
The **Access Control** window appears.
2. Click the **Directory Settings** tab.
PowerProtect Data Manager displays a list of configured identity providers.
3. Click **Add**.
The **Add Directory** window appears.
4. Configure the following attributes:

Table 7. Identity provider attributes

Attribute	Description
Server Type	Select a supported identity provider type.
Server Address	Type the hostname or IP address of the identity provider. A protocol prefix is not required.
Secure Connection	Select this attribute if the identity provider uses a secure connection method such as LDAPS or AD over SSL. Selecting this attribute enables the certificate validation controls.
Port	Type the port number for the identity provider.
Domain	Type the domain for which this identity provider authenticates users. For example, ldap.example.com .
User Name	Type a user account that has full read access to the directory. A domain is not required.
Password	Type the password for the specified user account.

Table 7. Identity provider attributes (continued)

Attribute	Description
Group Search Attribute	Type the attribute name that the identity provider should use to validate the group name in the hierarchy.
Group Member Attribute	Type the attribute name that the identity provider should use to validate the group member in the hierarchy.
Group Search Base	If searches should not start from the default base, type the name of a base from which searches should start. Otherwise, leave this attribute empty. Separate multiple search bases with semicolons.

Populate the default values from this table into the appropriate fields when indicated:

Table 8. Default attribute values

Attribute	Value or format	
	AD and AD over SSL	LDAP and LDAPS
Port	<ul style="list-style-type: none"> For unsecure connections, the default port number is 389. For secure connections, the default port number is 636. 	
Group Search Attribute	sAMAccountName	cn
Group Member Attribute	member	memberUid

5. If you selected a secure connection method:
 - a. Click **Verify**.
 - b. In the **Verify Certificate** window, verify the details of the identity provider TLS certificate and then click **Accept**.

NOTE: When you specify the LDAPS protocol, PowerProtect Data Manager automatically downloads the certificates required to connect to the identity provider. Once downloaded, the **Certificate Validation** field appears. Click **Verify** to compare the displayed certificate information with the expected certificate information. If the certificates match, click **Accept** to continue with the setup. Otherwise, click **Cancel** to cancel the setup.
6. Click **Save**.


Next steps

Assign identity provider groups to a role. The section [Add identity provider group-to-role mapping](#) on page 34 provides instructions. You cannot log in as an external user without mapping users or groups to roles.

Edit an external identity provider

Only the Administrator and the Security Administrator roles can edit an external identity provider.

Steps

1. From the left navigation pane, select **Administration > Access Control**.
The **Access Control** window appears.
2. Click the **Directory Settings** tab.
PowerProtect Data Manager displays a list of configured identity providers.
3. To view more information about an identity provider, click  in the **Details** column for that identity provider.
PowerProtect Data Manager opens the **Details** pane, which displays information about the identity provider's configuration.
4. Select the identity provider, and then click **Edit**.
5. Edit the attributes as required.
6. Click **Save**.

Delete an external identity provider

Only the Administrator and the Security Administrator roles can delete an external identity provider.

Steps

1. From the left navigation pane, select **Administration > Access Control**.
The **Access Control** window appears.
2. Click the **Directory Settings** tab.
PowerProtect Data Manager displays a list of configured identity providers.
3. Select the identity provider that you would like to delete, and then click **Delete**.

Managing user roles and privileges

Users are defined by the local identity provider or by an external identity provider. Users and groups can access all protection policies and assets within the PowerProtect Data Manager environment.


A user's assigned role defines the associated privileges and determines the tasks that the user can perform.

Managing local identity provider users

The following topics describe basic user management for the local identity provider. Only the Administrator and the Security Administrator roles can manage users. The Administrator, Security Administrator, and User roles can view users.

An identity provider is an abstract source of user and group data that PowerProtect Data Manager can map to corresponding roles. An identity provider can be internal to PowerProtect Data Manager or external, such as a supported directory service. PowerProtect Data Manager queries an identity provider to authenticate users as part of the log-in process.

The *PowerProtect Data Manager Security Configuration Guide* provides more information about identity providers, including configuration, role-mapping, and external users. The *PowerProtect Data Manager Security Configuration Guide* also provides information about the local identity provider.

 **NOTE:** User authorization grants or denies users access to PowerProtect Data Manager resources. Authorization is the same for local identity provider users and external identity provider 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 local user

Only the Administrator and the Security Administrator roles can add users to the local identity provider.

Steps

1. From the left navigation pane, select **Administration > Access Control**.
The **Access Control** window appears.
2. Click the **Users/Groups** tab.
PowerProtect Data Manager displays a list of configured user accounts and external identity provider groups, including any associated roles.
3. Click **Add User/Group**.
The **Add User/Group** window opens.
4. Select **Local User**.
5. Provide the following information:
 - **First Name**
 - **Last Name**
 - **User Name**
 - **Email Address**
 - **Password**

- Retype to confirm the password.
- **Force Password Change**—Enabled by default. Requires the user to update the password at first login.
- **Role**

6. Click **Save**.


Results

The new user appears in the list of configured user accounts.

Edit or delete a local user

Only the Administrator and the Security Administrator roles can edit or delete local identity provider users.

Steps

1. From the left navigation pane, select **Administration > Access Control**.
The **Access Control** window appears.
2. Click the **Users/Groups** tab.
PowerProtect Data Manager displays a list of configured user accounts and external identity provider groups, including any associated roles.
3. Click  for any user account to see the following information:
 - Username
 - First name
 - Last name
 - Email address
 - User role
 - Date the user was created
4. Select the user that you want to edit or delete.
5. 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 list of configured user accounts.

Common password policy

When you set a local identity provider account password, ensure that the credential meets the following requirements:

- Contains a minimum of nine characters and a maximum of one hundred characters
- Contains at least one numeric character (0-9)
- Contains at least one uppercase character (A-Z)
- Contains at least one lowercase character (a-z)
- Contains at least one special character from the following list of acceptable characters:

!@#\$%^&*()-_+=~{ } [] < > ? / ` ' , . | \ " ' "

Spaces are allowed.

- Contains only letters from the English alphabet
- Does not contain other sensitive information that is associated with the user account, such as the first and last names, username, or email address

Change a local user password

Use the self-service feature to change the password for a local identity provider user.

Prerequisites

If you do not know the current password, [Reset a forgotten local user password](#) on page 27 provides more information. External identity provider users cannot reset their password using this procedure. Contact the identity provider administrator to reset your password.

Steps

1. Log in to the PowerProtect Data Manager UI.
2. From the banner, select **User Options > Change Password**.
3. Type the current password for the local user.
4. Type the new password twice for confirmation.
The new password must conform to the [Common password policy](#) on page 26.
5. Click **Save**.

Reset a forgotten local user password

Use the self-service feature to reset a forgotten password for a local user.

Prerequisites

- The account must be a local identity provider user.
- A mail server must be configured on PowerProtect Data Manager.
- External identity provider users cannot reset their password using this procedure. Contact the identity provider administrator to reset your password.

Review [Common password policy](#) on page 26 before you select a new 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.

Steps

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.

Reset operating system passwords


Only the Administrator role can reset operating system passwords. You can change the password for the Linux operating system root, admin, and support users by using the PowerProtect Data Manager UI.

About this task

For the root user, this method works if the current password has not expired and you know the current password. If the password has expired, the attempt fails.

Review [Common password policy](#) on page 26 before you select a new password.

Steps

1. Log in to the PowerProtect Data Manager user interface as a user with the Administrator role.
2. Click , and then select **Authentication**. The **System Users** window displays.
3. Select the password you want to change:
 - For the root and support users, click **Edit**.
 - For the operating system admin user, click **Reset**. You can reset the operating system admin user password without providing the existing password.
4. Update the form, and then click **Save**.

Default authorizations

Take note of the following user, group, and role considerations when authorizing users or adding users to roles and groups.

Default admin user

The default admin user is preassigned the Administrator 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.

Oracle group users

Note that users in the Oracle group have permission to delete the lockbox configuration file. To prevent data loss, add only trusted users to this group.

System-provided roles and associated privileges

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.

By using the predefined roles, you can limit access to PowerProtect Data Manager and to backup data by applying the principle of least privilege.

You can assign a user to multiple roles. For example, a user who has both Backup Administrator and Restore Administrator roles but does not have full system administration privileges.

Administrator role

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

User role

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. Users with this role do not require the ability to configure the system or access backup data. Most privileges that are held by this role are read-only.

Security Administrator role

The Security Administrator role is defined for a limited set of users whose manage user accounts and roles, privileges, audit logs, and authentication sources. These functions are separate from the Administrator role. You can assign this role to individuals with security clearances who may not be responsible for day-to-day operations but who clear other users for access.

Backup Administrator role

The Backup Administrator role is responsible for defining, configuring, and completing protection tasks such as backup operations. Individuals with this limited access role do not require the full set of system administrator permissions. These users work with resources that the system administrator has already configured. The Backup Administrator role can backup assets and manage copies at the asset level but cannot back up at the protection policy level.

Restore Administrator role

The Restore Administrator role is responsible for completing restore operations. Individuals with this limited access role do not require the full set of system administrator permissions. These individuals work with backups that exist in protection storage and with resources that the system administrator has already configured.

Role privileges

The following table details the privileges that correspond to each predefined role. [Role privilege definitions](#) on page 31 provides more information about the allowed activities for each privilege.

Table 9. Role privileges

Category	Roles				
	Administrator	User	Security Administrator	Backup Administrator	Restore Administrator
Monitoring					
View Events	Y	Y	N	Y	Y
Manage Events	Y	N	N	Y	Y
View Historical Data	Y	Y	N	N	N
View Task/Activities	Y	Y	N	Y	Y
Manage External Notifications	Y	N	N	N	N
Security and System Audit					
View Security/System Audit	Y	Y	Y	N	N
Manage Security/System Audit	Y	N	Y	N	N
User and Security Management					
View User Security	Y	Y	Y	N	N
Manage User Security	Y	N	Y	N	N
Support Assistance and Log Management					
View Diagnostic Logs	Y	Y	N	N	N
Manage Diagnostic Logs	Y	N	N	N	N
System Management					
View System Settings	Y	Y	Y	Y	Y

Table 9. Role privileges (continued)

Category	Roles				
Privilege	Administrator	User	Security Administrator	Backup Administrator	Restore Administrator
Manage System Settings	Y	N	N	N	N
Activity Management					
Manage Task	Y	N	N	Y	Y
Workflow Execution	Y	N	N	N	N
Manage Discovery Jobs	Y	N	N	N	N
Asset Management					
View Assets	Y	Y	Y	Y	Y
Manage Assets	Y	N	N	Y	N
View Asset Sources	Y	Y	N	Y	Y
Manage Asset Sources	Y	N	N	N	N
View Host	Y	Y	N	Y	Y
Manage Host	Y	N	N	N	Y
View Protection Engines	Y	Y	N	Y	Y
Manage Protection Engines	Y	N	N	N	N
View Search Engines	Y	Y	N	Y	Y
Manage Search Engines	Y	N	N	N	N
Storage Management					
View Protection Storage Targets	Y	Y	N	Y	Y
Manage Protection Storage Targets	Y	N	N	N	N
View Storage Array	Y	Y	N	Y	Y
Manage Storage Array	Y	N	N	N	N
Manage Network	Y	N	N	N	N
Protection Policy					
View Policies	Y	Y	N	Y	N
Manage Policies	Y	N	N	N	N
Recovery and Reuse Management					
Rollback to Production	Y	N	N	N	Y
Recovery to Alternate Location	Y	N	N	N	Y
Export for Reuse	Y	N	N	N	Y
SLA Compliance Management					
View SLA/SLO	Y	N	N	Y	N
Manage SLA/SLO	Y	N	N	N	N
Copy Management					
View Copies	Y	N	N	Y	Y

Table 9. Role privileges (continued)

Category	Roles				
	Administrator	User	Security Administrator	Backup Administrator	Restore Administrator
Manage Copies	Y	N	N	Y	N
View Retention Range	Y	N	N	Y	N
Manage Retention Range	Y	N	N	N	N
Delete Copies	Y	N	N	N	N
All Copies Search	Y	N	N	N	N
Resource Group					
View Resource Groups	Y	N	Y	N	N
Manage Resource Groups	Y	N	Y	N	N

Role privilege definitions

[System-provided roles and associated privileges](#) on page 28 lists the privileges that PowerProtect Data Manager associates with each integrated role. For each privilege, the following tables identify the specific tasks which a user with that privilege can perform.

Table 10. Monitoring privileges

Privilege	Task
View Events	<ul style="list-style-type: none"> View alerts and external notifications.
Manage Events	<ul style="list-style-type: none"> Create, publish, cancel, ignore, promote, and demote alerts and external notifications.
View Historical Data	<ul style="list-style-type: none"> View historical data that relates to plans, arrays, data targets, data sources, and capacity data.
View Tasks or Activities	<ul style="list-style-type: none"> View task resources.
Manage External Notifications	<ul style="list-style-type: none"> Subscribe or unsubscribe a user for alert notifications.

Table 11. Security and system audit privileges

Privilege	Task
View Security/System Audit	<ul style="list-style-type: none"> View security audit–related events and activities.
Manage Security/System Audit	<ul style="list-style-type: none"> Acknowledge security audit–related events and activities. Export audit/change log of events and activities.

Table 12. Support assistance and log management privileges

Privilege	Task
View Diagnostic Logs	<ul style="list-style-type: none"> View log bundle resources. View log information resources. View the log source resource. View logs.
Manage Diagnostic Logs	<ul style="list-style-type: none"> View and manage log bundle resources. View and edit the log source resource. Export logs.

Table 13. User and security management privileges

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

Table 14. System management privileges

Privilege	Task
View System Settings	<ul style="list-style-type: none"> • View server disaster recovery artifacts. • View maintenance mode. • View license information. • View server disaster recovery status. • View SupportAssist information. • View node, configuration EULA, operating system user, update package, component, configuration status, configuration logs, time zone, and state resources.
Manage System Settings	<ul style="list-style-type: none"> • Manage server disaster recovery activities. • Manage SupportAssist gateway connection and other telemetry communications. • View and edit node state resources. • Update license information. • View component, configuration status, configuration logs, time zone, and state resources. • View and edit node, configuration EULA, operating system user, and lockbox resources. • Create, view, edit, and delete update package resources.

Table 15. Activity management privileges

Privilege	Task
Manage Task	<ul style="list-style-type: none"> • Create, view, edit, and cancel activity resources.
Workflow Execution	<ul style="list-style-type: none"> • Start and cancel workflow execution. • View the status of workflow execution.
Manage Discovery Jobs	<ul style="list-style-type: none"> • Create, view, edit, and delete discovery jobs.

Table 16. Asset management privileges

Privilege	Task
View Assets	<ul style="list-style-type: none"> • View assets.
Manage Assets	<ul style="list-style-type: none"> • Create, view, edit, and delete assets.
View Asset Sources	<ul style="list-style-type: none"> • View asset sources.
Manage Asset Sources	<ul style="list-style-type: none"> • Create, view, edit, and delete asset sources.
View Host	<ul style="list-style-type: none"> • View asset hosts.
Manage Host	<ul style="list-style-type: none"> • Create, view, edit, and delete asset hosts.
View Protection Engines	<ul style="list-style-type: none"> • View protection engines.
Manage Protection Engines	<ul style="list-style-type: none"> • Create, view, edit, and delete protection engines.
View Search Engine	<ul style="list-style-type: none"> • View the Search Engine.
Manage Search Engine	<ul style="list-style-type: none"> • Create, view, edit, and delete the Search Engine.

Table 17. Storage management privileges

Privilege	Task
View Protection Storage Targets	<ul style="list-style-type: none"> View storage targets.
Manage Protection Storage Targets	<ul style="list-style-type: none"> Create, view, edit, and delete storage targets.
View Storage Array	<ul style="list-style-type: none"> View storage arrays.
Manage Storage Array	<ul style="list-style-type: none"> Create, view, edit, and delete storage arrays.
Manage Network	<ul style="list-style-type: none"> Assign network interfaces to storage arrays.

Table 18. Protection policy privileges

Privilege	Task
View Policies	<ul style="list-style-type: none"> View a list of all protection policies. View the storage targets of protection policy. View the accessible assets that are assigned to protection policies. View protection policy schedules. View protection policy networking and other advanced options. View file filters. View protection rules.
Manage Policies	<ul style="list-style-type: none"> Create, view, edit, and delete protection policies. Disable protection policies. Create, view, edit, and delete schedule resources. Add, view, and edit protection policy storage targets. Add, view, and edit protection policy assets. Perform manual backups of protected assets. Create, view, edit, and delete file filters. Create, view, edit, and delete protection rules filters. Assign network interfaces.

Table 19. Recovery and reuse management privileges

Privilege	Task
Rollback to Production	<ul style="list-style-type: none"> Create, view, edit, and start restore to production operations. Create, view, edit, and delete resources that are related to media manager assets.
Recovery to Alternate Location	<ul style="list-style-type: none"> Create, view, edit, and start restore to alternate location operations. Create, view, edit, and delete resources that are related to media manager assets.
Export for Reuse	<ul style="list-style-type: none"> Create, view, edit, and start export and reuse operations. Create, view, edit, and delete resources that are related to media manager assets.

Table 20. SLA compliance management privileges

Privilege	Task
View SLA/SLO	<ul style="list-style-type: none"> View compliance results.
Manage SLA/SLO	<ul style="list-style-type: none"> Create, view, edit, delete, and export compliance results.

Table 21. Copy management privileges

Privilege	Task
View Copies	<ul style="list-style-type: none"> View asset copies and backups.
Manage Copies	<ul style="list-style-type: none"> Edit asset copy and backup retention. Recall copies from the cloud.

Table 21. Copy management privileges (continued)

Privilege	Task
	<ul style="list-style-type: none"> Edit asset copy and backup recall retention.
View Retention Range	<ul style="list-style-type: none"> View retention range.
Manage Retention Range	<ul style="list-style-type: none"> Manage retention range across all copies and backups.
Delete Copies	<ul style="list-style-type: none"> Delete copies and backups.
All Copies Search	<ul style="list-style-type: none"> Manage available copies and backups.

Table 22. Resource group privileges

Privilege	Task
View Resource Groups	<ul style="list-style-type: none"> View a list of all resource groups. View resource group details.
Manage Resource Groups	<ul style="list-style-type: none"> Create, view, edit, and delete resource groups.

External authorization associations

This section describes how to connect PowerProtect Data Manager authorization to identity provider-based subjects.

Add identity provider group-to-role mapping

Only the Administrator and the Security Administrator roles can add identity provider group-to-role mapping.

Steps

- From the left navigation pane, select **Administration > Access Control**.
The **Access Control** window appears.
- Click the **Users/Groups** tab.
PowerProtect Data Manager displays a list of configured user accounts and external identity provider groups, including any associated roles.
- Click **Add User/Group**.
The **Add User/Group** window opens.
- Select **AD/LDAP User Group**.
- Select the domain which corresponds to the identity provider for which you would like to add group-to-role mapping.
- In **Groups**, start typing the name of a identity provider group.
PowerProtect Data Manager searches the identity provider and displays any matching groups.
- Select one or more groups from the list of results.
- Select one or more roles for all group users.
- Click **Add**.


Modify identity provider group-to-role mapping

Only the Administrator and the Security Administrator roles can modify identity provider group-to-role mapping.

Steps

- From the left navigation pane, select **Administration > Access Control**.
The **Access Control** window appears.
- Click the **Users/Groups** tab.

PowerProtect Data Manager displays a list of configured user accounts and external identity provider groups, including any associated roles.

3. Click  for any group to see the following information:
 - Group name
 - Group type
 - Group role
 - Date the group was mapped
4. Select the group that you want to edit, and then click **Edit**.
The **Edit User/Group** window opens.
5. Assign the group to a different role.
The domain and group name are read-only.
6. Click **Save**.

Delete identity provider group-to-role mapping

Only the Administrator and the Security Administrator roles can delete identity provider group-to-role mapping.

Steps

1. From the left navigation pane, select **Administration > Access Control**.
The **Access Control** window appears.
2. Click the **Users/Groups** tab.
PowerProtect Data Manager displays a list of configured user accounts and external identity provider groups, including any associated roles.
3. Select the group that you want to delete, and then click **Delete**.
4. Click **OK** to confirm the deletion.

Remote component authentication

The PowerProtect Data Manager lockbox securely stores known secrets. These secrets include any user account and protection storage credentials that you supply as you configure the software.

[Credential security](#) on page 37 provides more information about the lockbox.

PowerProtect Data Manager can use stored credentials in multiple contexts. The term "consumer" means a place where the appliance uses a credential, for any purpose. For example:

- A username and password may apply to one individual host or asset. In this case, the host or asset is the consumer.
- The same credential could also apply to all assets on the same protection policy, if the assets all authenticate with the same username and password. In this case, the protection policy is the consumer, even though the credential applies to the assets under that policy.

You can manage stored credentials through the PowerProtect Data Manager UI or the REST API.

Add a credential

Supply PowerProtect Data Manager with the necessary credentials to access external systems, such as storage targets, assets, and asset sources. You can also add credentials when you create a protection policy.

Steps

1. From the left navigation pane, select **Administration > Credentials**.
The **Credentials** window appears.
2. Click **Add**.
The **Add Credential** dialog box opens.
3. Type a name for the credential.
Credential names should clearly identify the intended purpose and usage.

4. Select a credential type from the drop-down list.
The credential type determines the remaining fields. For example, username and password, token, or key.
5. Complete the remaining fields according to the selected type.
6. Click **Save**.
PowerProtect Data Manager adds the credential to the keystore.

View credential usage

For each stored credential, you can see a list of items that use that credential.

Steps

1. From the left navigation pane, select **Administration > Credentials**.
The **Credentials** window appears.
2. Locate the credential in the list of stored credentials.
Use the filters and column sort options to organize the list of credentials.
3. Select the credential from the list.
Review the **Consumer Count** column for that credential. If the count is zero, the credential is not used anywhere.
4. Select the number in the **Consumer Count** column.
The **Details** pane opens and displays a list of consumers that use the selected credential. The list groups items by type. For example, assets, protection policies, or storage targets.

Edit a credential

You can change a credential name or stored authentication details, such as a username or password. You cannot change the credential type.

Steps

1. From the left navigation pane, select **Administration > Credentials**.
The **Credentials** window appears.
2. Locate the credential in the list of stored credentials.
Use the filters and column sort options to organize the list of credentials.
3. Select the credential from the list, and then click **Edit**.
The **Edit Credential** dialog box opens.
4. Modify any appropriate values.
The available values depend on the credential type. For example, username and password, token, or key.
5. Click **Save**.
PowerProtect Data Manager updates the stored credential.

Delete credentials

You can delete any credentials that are no longer in use or which you no longer need. Deleting a credential creates an entry in the audit log.

Prerequisites

The credentials must not be used anywhere. Verify the credential usage and that the consumer count is zero. If necessary, update anything that uses the credentials, such as protection policies or assets.

Steps

1. From the left navigation pane, select **Administration > Credentials**.
The **Credentials** window appears.
2. Locate the credential in the list of stored credentials.

Use the filters and column sort options to organize the list of credentials.

3. Select the credential or credentials from the list.
4. Verify that the **Consumer Count** column displays zero consumers.
If the count is zero, the credential is not used anywhere and you can delete the credential. The **Delete** button activates when all selected credentials have zero consumers.
5. Click **Delete**.
6. Click **OK** to confirm the deletion.
PowerProtect Data Manager removes the credential.

Credential security

The PowerProtect Data Manager lockbox securely stores known secrets in a central location.

All stored secrets in the lockbox are encrypted. When an activity requires information from the lockbox, the requesting process provides the lockbox passphrase and then receives the required information in a decrypted format.

The lockbox holds secrets such as:

- Credentials for local user accounts.
- Protection storage credentials that you supply as you configure the appliance.
- Credentials by which application agents authenticate to protected assets.

PowerProtect Data Manager creates a strong, unique passphrase during deployment to protect the lockbox contents. After deployment, PowerProtect Data Manager automatically encrypts and manages the lockbox passphrase without user interaction. Automatic management removes the requirement to provide the lockbox passphrase when you update from supported releases. Server DR backups protect the lockbox and its contents.

The File System agent also uses a separate lockbox on protected hosts to store sensitive information, including the credentials by which the application agent accesses external storage infrastructure.

For Kubernetes, PowerProtect Data Manager stores the necessary certificates and credentials for protection operations in a secret resource on the Kubernetes cluster. The [Kubernetes documentation](#) provides more information about how to enable encryption for this secret resource.

Managing Storage

Topics:

- [Protection storage](#)
- [Storage units](#)
- [Overview of PowerProtect Data Manager Cloud Tier](#)

Protection storage

Protection storage is the set of configured storage systems where PowerProtect Data Manager stores backup copies, replicated copies, and other important information. Protection storage can include any of the following:

- A DD system, including High Availability PowerProtect DD mode
- An instance of PowerProtect DD Management Center that manages multiple DD systems

NOTE: Data Domain is now PowerProtect DD. References to Data Domain or DD systems in this documentation, in the UI, and elsewhere in the product include PowerProtect DD systems and older Data Domain systems. In many cases the UI has not yet been updated to reflect this change.

The most up-to-date software compatibility information for PowerProtect Data Manager is provided in the [eLab Navigator](#).

Observe the following information before you configure protection storage:

- Adding and configuring protection storage requires the Administrator role.
- You cannot add protection storage that runs incompatible versions of DDOS.
- You can only add the same protection storage system once, whether you specify the hostname, FQDN, or IP address.
- You cannot add a PowerProtect DD Management Center instance which has no managed DD systems.

Protection storage is further divided into logical groupings that are called storage units, which hold related data and apply more detailed configuration options.

NOTE: Adding a PowerProtect DD Management Center instance is not required for the Storage Direct agent.

PowerProtect DD Management Center automatic discovery

When you add an instance of PowerProtect DD Management Center, PowerProtect Data Manager automatically discovers all the supported DD systems which that PowerProtect DD Management Center instance manages.

PowerProtect Data Manager displays the discovered DD systems on the **Protection Storage** tab of the **Infrastructure > Storage** window after discovery finishes. It may take a few minutes for the discovered systems to appear.

For each DD system, the **Managed By** column in the table indicates the PowerProtect DD Management Center instance that manages the DD system.

If you add a DD system directly to PowerProtect Data Manager, the **Managed By** column displays the name that you provided for the DD system.

High Availability PowerProtect DD support

PowerProtect Data Manager supports DD systems with High Availability (HA) enabled. The Active-Standby configuration provides redundancy in the event of a system failure. HA keeps the active and standby systems synchronized, so that if the active node were to fail, the standby node can take over services and continue where the failing node left off.

When an active High Availability PowerProtect DD system fails over to its standby High Availability PowerProtect DD system, all in progress PowerProtect Data Manager operations including backup, restore, replication, and Cloud Tier continue unaffected.

To add a High Availability PowerProtect DD configuration as a storage target in PowerProtect Data Manager, select **Infrastructure > Storage** in the PowerProtect Data Manager UI. [Add protection storage](#) on page 39 provides more information.

Virtual machine application-aware protection are only be supported with DDOS version 7.0 or later for HA. The most up-to-date software compatibility information for PowerProtect Data Manager is provided in the [eLab Navigator](#).

For details on DD systems with HA enabled, see the *DDOS Administration Guide*.

Add protection storage

Add and configure a storage system to use as a target for protection policies. Only the Administrator role can add protection storage.

Prerequisites

NOTE:

When adding a High Availability PowerProtect DD system, observe the following points:

- Do not add the individual active and standby DD systems to PowerProtect Data Manager.
- In the **Address** field, use the hostname that corresponds to the floating IP address of the High Availability PowerProtect DD system.
- The High Availability PowerProtect DD system is verified with the root certificate.

Steps

1. From the left navigation pane, 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 (**PowerProtect DD System** or **PowerProtect DD Management Center**).
4. To add a High Availability PowerProtect DD system, select the checkbox.
5. 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.
 - c. In the **Port** field, specify the port for SSL communication. Default is 3009.
6. Under **Host Credentials** click **Add**, if you have already configured protection storage credentials that are common across storage systems, select an existing password. Alternatively, you can add new credentials, and then click **Save**.
7. If a trusted certificate does not exist on the storage system, a dialog box appears requesting certificate approval. Click **Verify** to review the certificate, and then click **Accept**.
8. 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.
9. 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**.
10. To modify a storage system location, complete the following steps:

A storage system location is a label that is applied to a storage system. If you want to store your copies in a specific location, the label helps you select the correct storage system during policy creation.

 - a. In the **Storage** window, select the storage system from the table.
 - b. Click **More Actions > Set Location**.
The **Set Location** window appears.
 - c. Click **Add** in the **Location** list.
The **Add Location** window appears.
 - d. In the **Name** field, type a location name for the asset, and click **Save**.

Results

PowerProtect Data Manager displays external DD systems only in the **Storage** window **Name** column. PowerProtect Data Manager displays PowerProtect DD Management Center storage types in the **Managed By** column.

Edit protection storage

You can change the name, port number, and credentials for an existing protection storage system. You cannot change the address. Only the Administrator role can edit protection storage.

Steps

1. From the left navigation pane, select **Infrastructure > Storage**.
The **Storage** window appears.
2. In the **Protection Storage** tab, select a protection storage system and then click **Edit**.
3. In the **Edit Storage** dialog box, specify the storage system attributes:
 - a. In the **Name** field, specify a new storage name.
 - b. In the **Port** field, specify the port for SSL communication. Default is 3009.
 - c. Under **Host Credentials**, select a new set of credentials or click **Add**.
4. If a trusted certificate does not exist on the storage system, a dialog box appears requesting certificate approval. Click **Verify** to review the certificate, and then click **Accept**.
5. Click **Save** to exit the **Add Storage** dialog.

Storage units

PowerProtect Data Manager can create, configure, and reuse storage units on a protection storage system. These storage units are the targets for protection and replication policies.

The term "storage unit under the control of PowerProtect Data Manager" describes a storage unit that was created through one of the methods that are discussed here.

Review the applicable limitations before you create or change a storage unit, or change the protection or replication target for a policy. The *PowerProtect DD Virtual Edition Installation and Administration Guide* for the appropriate platform provides more information about storage units (MTrees).

Storage unit creation and configuration

PowerProtect Data Manager provides two ways to create storage units on the protection storage system:

- If you do not select an existing storage unit when you create a protection policy, PowerProtect Data Manager automatically creates a storage unit for you.
- Through the PowerProtect Data Manager UI, you can directly create storage units as required.

You can use the UI to configure the quotas and credentials for storage units under the control of PowerProtect Data Manager.

Storage unit selection

When you create or edit a protection policy, PowerProtect Data Manager provides the option to select a storage unit as the protection or replication target. The storage unit can be on the same or another protection storage system.

The **Storage** page lists all storage units that were discovered on a protection storage system. Only storage units under the control of PowerProtect Data Manager are available to select for a protection policy. Other storage units are not available to select, even if known.

A storage unit under the control of PowerProtect Data Manager can be the target for multiple protection policies. When you select an existing storage unit as a policy target, the policy inherits the storage unit's quota settings.

[Managing Protection Policies](#) on page 73 provides more information about using storage units with policies.

Security

All protection policies and applications that share a storage unit can access any data in that storage unit. Reuse a storage unit only for policies and applications that belong to the same organizational unit or which share a trusted relationship. Policies and applications for different organizational units should use different storage units.

Any other external applications that also use the storage unit should protect and restrict access to the DD Boost credentials. These credentials provide access to the PowerProtect Data Manager data.

Automatic storage unit maintenance

For automatically-created storage units, automatic maintenance removes the storage unit when both the following conditions are true:

- No protection policies target the storage unit for backups or replication.
- The storage unit contains no backups.

Automatic maintenance removes these empty, unused storage units even if retention lock is enabled.

For directly-created storage units, automatic maintenance does not remove the storage unit even when these conditions are true. In this case, contact the protection storage system administrator to remove the storage units.

Updating from previous releases

Any protection policy can use storage units that were automatically created for policies in a previous release of PowerProtect Data Manager. Policies that were created in a previous release continue to function as before.

Previous releases of the Oracle agent do not support storage units with multiple protection policies. The *PowerProtect Data Manager for Oracle RMAN Agent User Guide* provides more information.

Storage unit limitations

When using storage units with multiple protection policies, the following limitations apply:

- PowerProtect Data Manager cannot target or configure storage units that were not created through PowerProtect Data Manager.
- PowerProtect Data Manager cannot target storage units that were configured elsewhere for Cloud Tiering.
- Moving a protection policy to another storage unit or protection storage system may require a full backup.
 - For virtual machines, file system backups, Kubernetes, and Exchange, the next backup is automatically promoted to a full backup.
 - For SQL, Oracle, and SAP HANA backups, complete a manual full backup of these assets with the new storage unit.
- Protection policies for Storage Data Management cannot share a storage unit with other protection policies.
- Retention lock on a storage unit is disabled if any protection policy on that storage unit has retention lock disabled.
- Previous releases of the Oracle agent do not support sharing a storage unit between protection policies. The *PowerProtect Data Manager for Oracle RMAN Agent User Guide* provides more information.

Storage unit considerations for PowerProtect DD

With respect to PowerProtect DD, storage units have certain restrictions and best practices. Be aware of the following considerations:

- In order to avoid synchronization issues with PowerProtect Data Manager, any storage units that PowerProtect Data Manager is managing or using should not be deleted directly from the DD.
- Storage units that you create in PowerProtect Data Manager must not be changed by the DD administrator to set up storage unit replication.
- Storage units that you create in PowerProtect Data Manager must not be configured for Cloud Tiering.
- The following limitations apply to the number of supported storage units by PowerProtect DD model:

Table 23. Supported storage units for PowerProtect DD Operating System (DDOS) versions

PowerProtect DD system	DDOS version	Maximum number of storage units supported	Supported configurable concurrently active storage units
DD9800	6.0 and later	256	256
DD9500	5.7 and later	256	256
DD6800, DD9300	6.0 and later	128	128

Table 23. Supported storage units for PowerProtect DD Operating System (DDOS) versions (continued)

PowerProtect DD system	DDOS version	Maximum number of storage units supported	Supported configurable concurrently active storage units
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 24. Supported storage units in PowerProtect DD Virtual Edition (DDVE) by TB

Number of TBs	Maximum number of storage units	Supported configurable concurrently active storage units
4	100	6
6		
8		
32	100	14
48		
64	100	32
96		

Create a storage unit

Directly create a storage unit through the PowerProtect Data Manager UI for use with protection policies.

Prerequisites

Add at least one protection storage system for PowerProtect Data Manager.

Steps

- From the left navigation pane, select **Infrastructure > Storage**.
The **Storage** window appears.
- On the **Protection Storage** tab, select a storage system, and then select **More Actions > Manage Storage Units**.
The **Storage Units** page opens and displays a list of the storage units under the control of PowerProtect Data Manager.
- Select **Add**.
The **Create Storage Unit** dialog box opens.
- Type a name for the new storage unit and then select a set of credentials.
Alternatively, you can select **Add Credentials** from the list to add new credentials. Provide a descriptive name for the credentials, a username, and a password. Then, click **Save** to store the credentials.
- Set the capacity and stream quotas that restrict the storage unit resource consumption.
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. When you set a hard limit and the limit is reached, data cannot be written. All data protection operations fail until data is deleted

from the storage unit. The *PowerProtect DD Virtual Edition Installation and Administration Guide* for the appropriate platform provides more information about quota configuration.

- a. **Capacity Quota**—Controls the total size of precompression data that is written to the protection storage.
- b. **Stream Quota**—The number of concurrent streams allowed during data protection operations. Setting a **Stream Quota** limit can help ensure that performance is not impacted negatively when a data protection operation consumes too many resources.

6. Select **Save**.

Results

PowerProtect Data Manager creates the storage unit on the selected protection storage system.


Edit a storage unit


Configure the quota settings for an existing storage unit through the PowerProtect Data Manager UI. You can also view a list of protection policies that target the storage unit.

About this task

Any changes to these storage unit attributes that you make directly on the protection storage system are also reflected in PowerProtect Data Manager.

Steps

1. From the left navigation pane, select **Infrastructure > Storage**.
The **Storage** window appears.
2. On the **Protection Storage** tab, select a storage system, and then select **More Actions > Manage Storage Units**.
The **Storage Units** page opens and displays a list of the storage units under the control of PowerProtect Data Manager.
3. To view the details or usage for a storage unit, select  for that storage unit.
The **Details** pane opens and displays the name, type, capacity, quota information, and a list of protection policies that currently target the storage unit.
The storage unit may contain copies from protection policies that no longer target the storage unit.
4. Select a storage unit from the list, and then select **Edit**.
The **Edit Storage Unit** dialog box opens.
5. Set the capacity and stream quotas that restrict the storage unit resource consumption.
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. When you set a hard limit and the limit is reached, data cannot be written. All data protection operations fail until data is deleted from the storage unit. The *PowerProtect DD Virtual Edition Installation and Administration Guide* for the appropriate platform provides more information about quota configuration.

- a. **Capacity Quota**—Controls the total size of precompression data that is written to the protection storage.
- b. **Stream Quota**—The number of concurrent streams allowed during data protection operations. Setting a **Stream Quota** limit can help ensure that performance is not impacted negatively when a data protection operation consumes too many resources.

6. Select **Save**.

Results

PowerProtect Data Manager updates the storage unit quota settings.

 **NOTE:** Ensure that the modified password policy complies with the DD password policy.

4. Restart the `cbs` service:
`cbs restart`
5. Verify that the `cbs` service started successfully.

Results

The modified password policy takes effect when the `cbs` service successfully starts.

View the storage unit password

PowerProtect Data Manager provides a script to retrieve the password for a storage unit that you configured as a backup target.

Prerequisites

This task requires the name of the PowerProtect DD MTree where the storage unit resides.

Steps

1. Connect to the PowerProtect Data Manager console as an admin user.
2. Navigate to the `/usr/local/brs/puppet/scripts` directory.
3. Obtain the storage unit password by typing the following command:
`./get_dd_mtree_credential.py MTree-name`

Overview of PowerProtect Data Manager Cloud Tier

The PowerProtect Data Manager Cloud Tier feature works in tandem with the Cloud Tier feature of DD systems to move PowerProtect Data Manager backups 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 protection storage to the cloud, and you can perform seamless recovery of these backups.

Cloud storage units must be pre-configured on the protection storage system before they are configured for Cloud Tier in the PowerProtect Data Manager UI. The *DDOS Administration Guide* provides further information.

Using the PowerProtect Search Engine

Topics:

- [Introducing the PowerProtect Search Engine](#)
- [Set up and manage indexing](#)
- [Search Engine node deletion](#)
- [Edit the network configuration for a search engine node](#)
- [Perform a search](#)
- [Virtual machine file level restore from a search](#)
- [Troubleshooting Search Engine issues](#)


Introducing the PowerProtect Search Engine

When you install PowerProtect Data Manager, the PowerProtect Search Engine software is installed by default.

The PowerProtect Search Engine indexes virtual machine file metadata to enable searches based on configurable parameters. To use this feature, add at least one search engine node to the Search Engine to form a search cluster. Adding a node enables the indexing feature.

You can enable the indexing option when creating protection policies so that the assets are indexed while they are backed up. Recovering indexes from a disaster is a manual process. [Recovering the Search Engine from a DR backup](#) on page 131 provides instructions. The indexing recovery process will be automated in a future release.

When a DR backup is run, scheduled, or manually triggered, the search cluster backup workflow backs up the cluster index data. A backup task is created, and you can view the individual status of the Search Component backup under **Details**.

 **NOTE:** Scheduled backups with Search cluster integration appear in the Jobs pane as two identical jobs: an initialization job, which runs immediately, and the backup job, which runs both ServerDR and Search cluster backups.

Limitations

PowerProtect Search is an optional feature that can be enabled, set up, and configured for virtual machine backups and protection policies. When you enable this feature, a backup of the search Engine is taken as part of the server backup process. As of this release, you cannot disable these backups. Therefore, when **Search** is enabled, you must add the search engine node on the DD system that contains the ServerBackup MTree to the **Allow** list. Add the search node IP address or hostname to the client list for the NFS export.

After an update to PowerProtect Data Manager, with the search engine already configured, and the first time that you use the **Networks** page to add a virtual network to an environment, PowerProtect Data Manager does not automatically add the virtual network to the search engine. Instead, manually edit each node to add the virtual network. This action makes the search engine aware of virtual networks. Any subsequent new virtual networks are automatically added to the search engine.


Set up and manage indexing

Set up a search engine node and configure indexing.

Prerequisites

Ensure that:


- A vCenter datastore has been configured. [Add a VMware vCenter Server](#) on page 62 provides detailed steps for adding a vCenter Server as an asset source.
- PowerProtect Data Manager has discovered the networks for the vCenter Server.
- The following requirements for the PowerProtect Search Engine are met:

 **NOTE:** Each search engine node must meet the system requirements.

- CPU: 4 * 2 GHz (4 virtual sockets, 1 core for each socket)
- Memory: 8 GB RAM
- Disks: 3 disks (50 GB each) and 1 disk (1 TB)
- Internet Protocol: IPv4 only
- NIC: One vmxnet3 NIC with one port
- The PowerProtect Data Manager system is configured to use an NTP server. NTP server configuration is required to synchronize the time across the search nodes in a multi-node search cluster.

Steps

1. From the PowerProtect Data Manager UI, select **Infrastructure > Search Engine**, and then click **Add Node**.
2. In the **Add Search Engine Node** wizard, provide the required parameters.
 - **Hostname, IP Address, Gateway, DNS, and Netmask**—Note that only IPv4 addresses are supported.
 - **vCenter**—If you have added multiple vCenter Server instances, select the vCenter on which to deploy the search engine node.

 **NOTE:** Ensure that you do not select the internal vCenter Server.
 - **ESX Host/Cluster**—Select on which cluster or ESXi host you want to deploy the search engine node.
 - **Network**—Displays all the networks that are available under the selected ESXi Host/Cluster. For virtual networks (VLANs), this network carries management traffic.
 - **Data Store**—Displays all datastores that are accessible to the selected ESXi Host/Cluster.

3. Click **Next**.
The **Networks Configuration** page displays.

4. On the **Networks Configuration** page:

The **Networks Configuration** page configures the virtual network (VLAN) to use for backup data. To continue without virtual network configuration, leave the **Preferred Network Portgroup** selection blank and then click **Next**.

- a. From the **Preferred Network Portgroup** list, select a Virtual Guest Tagging (VGT) group.
VST (Virtual Switch Tagging) groups are not supported.

The list displays all virtual networks within the trunk range. If you select a portgroup that contains multiple networks, PowerProtect Data Manager automatically selects all networks. Individual networks cannot be selected.

A search engine node requires an IP address from the static IP pool for each selected virtual network. If there are not enough IP addresses in a pool, the wizard prompts you to supply additional addresses for that network.


- b. If required, type an available static IP address or IP address range in the **Additional IP Addresses** column for the indicated virtual network.

For convenience when working with multiple virtual networks, you can also use one of the **Auto Expand** options:

- **Expand Last IP**—The wizard increments the host portion of the last IP address in the static IP pool. Click **Apply**.
- **Same Last Digit**—The wizard adds the network portion of the IP address to the specified value. Type the host portion of the IP address and then click **Apply**.

The wizard updates the value in the **Additional IP addresses** column for each network. Verify the proposed IP addresses.

- c. Click **Next**.
5. On the **Summary** page, review the information and then click **Finish**.
The new search engine node is deployed, and details are displayed in the lower panel.
 6. (Optional) Repeat the previous steps to deploy additional search engine nodes to the search cluster.

 **NOTE:** Ensure that the previous search engine node has successfully deployed before you add another node.

7. In the **Configure Search Engine** dialog box, enable or disable Search Indexing, accept or change the expiration period, and then click **OK**.

 **NOTE:**

- When the index cluster reaches 70 percent, an alert is generated. When it reaches 90 percent, an alert is generated and indexing is suspended. Specify a global index expiry interval to periodically clean up indexes, which frees up space.

- To turn off or modify indexing, select **Infrastructure > Search Engine**, select the cluster, and click **Configure Cluster**. From the **Configure Search Cluster** dialog box, you can enable/disable the service or change the number of expiration days.
- Indexes expire according to the global setting or when the associated copies expire, whichever occurs first.
- To stop indexing assets that have been added to a protected protection policy, disable the indexing option during protection policy configuration.
- You can add up to a maximum of 5 search engine nodes.

Next steps

NOTE:

When you edit or retry an operation that failed and there are additional IP addresses in the address pool, PowerProtect Data Manager marks the last failed IP address as abandoned. PowerProtect Data Manager does not try to reuse any IP addresses that are marked as abandoned. The UI does not display this condition.

[KB article 000181120](#) provides more information about how to use the REST API to detect when an IP address is marked as abandoned. The article also provides steps to correct this condition so that the IP address can be used again.

Search Engine node deletion

PowerProtect Data Manager supports the deletion of a Search Engine node from a multi-node Search cluster in the PowerProtect Data Manager UI.

You can delete an operational node from a Search cluster to decrease cluster capacity if the space is no longer required. You can also redeploy or delete nodes that could not be successfully added to the Search Engine.

When you delete an operational node, PowerProtect Data Manager moves the index data to the remaining nodes to avoid data loss.

When you delete a node, the operation is triggered and a new job is created, which you can view in the **Jobs > System Jobs** window to track its progress.

Delete operational nodes from a Search cluster

You can delete nodes that have been added to PowerProtect Data Manager and are in an operational state.

About this task

Before you can delete the primary node, you must delete all other nodes.


 **CAUTION:** Deleting the primary node deletes the index data and makes the Search cluster inactive. Add a node to make the Search cluster operational.

Steps

1. From the PowerProtect Data Manager UI, select **Infrastructure > Search Engine**.
2. Select the node from the list that you want to delete and click **More Actions > Delete Node**.

In the **Delete Search Engine Node** window, choose one of the following options:

- Delete the node without data loss.
To delete the node and move the index data to the remaining nodes in the cluster, click **Delete Node**.
- Delete the node and its data.

 **CAUTION:** By selecting this option, the Search Engine deletes the node without redistributing the data to the remaining nodes in the cluster.

When you delete the node and the index data, the Search cluster becomes inactive.

To allow the Search Engine to delete the node along with the index data it holds, select the check box and click **Delete Node**.

3. Go to the **Jobs > System Jobs** window to monitor the progress of the node deletion operation.

Results

The node is deleted from the cluster.

Redeploy or delete failed nodes from a Search cluster

PowerProtect Data Manager enables you to redeploy or delete search nodes that could not be successfully deployed.

About this task

The **Redeploy Node** functionality is only enabled for nodes that could not be successfully added to the PowerProtect Search Engine.

Steps

1. From the PowerProtect Data Manager UI, select **Infrastructure > Search Engine**.
2. Select the failed node that you want to either redeploy or delete from the Search cluster.
3. Do one of the following:
 - To redeploy the failed node, click **More Actions > Redeploy Node**.
The **Redeploy Search Engine Node** wizard opens. The Search Engine populates the fields with the information that you supplied when you added the node. Verify that the information for the node is correct.
 - To delete the failed node, click **More Actions > Delete Node**.

Results

You can view the details for the operation in the **Jobs > System Jobs** window.

Next steps

Optionally, if you want to update the DNS and/or gateway during the search node redeployment, you can use one of the following commands:

- To update both the gateway and DNS, run `./infranodemgmt redeploy -node_id Search Node ID -updateDns DNS IPv4 address -updateGateway Gateway IPv4 address`
- To update the gateway only, run `./infranodemgmt redeploy -node_id Search Node ID -updateGateway Gateway IPv4 address`
- To update DNS only, run `./infranodemgmt redeploy -node_id Search Node ID -updateDns DNS IPv4 address`

Edit the network configuration for a search engine node

To change the virtual network configuration, perform the following steps. To change any other network configuration settings, contact Customer Support.

About this task

If search engine node deployment failed because of a virtual network configuration problem, you can update the configuration to add additional IP addresses to the static IP pool. If you did not configure a virtual network during initial deployment, you can also add the search engine node to a virtual network in the same Virtual Guest Tagging (VGT) port group.

Steps

1. From the PowerProtect Data Manager UI, select **Infrastructure > Search Engine** and then select the applicable search engine node.

2. Select **More Actions > Edit Networks**.

The **Edit Search Engine Node** wizard opens to the **Network Configuration** page.

3. If applicable, from the **Preferred Network Portgroup** list, select a VGT network.

The list displays all virtual networks within the trunk range. If you select a portgroup that contains multiple networks, PowerProtect Data Manager automatically selects all networks. Individual networks cannot be selected.

A search engine node requires an IP address from the static IP pool for each selected virtual network. If there are not enough IP addresses in a pool, the wizard prompts you to supply additional addresses for that network.

4. If required, type an available static IP address or IP address range in the **Additional IP Addresses** column for the indicated virtual network.

For convenience when working with multiple virtual networks, you can also use one of the **Auto Expand** options:

- **Expand Last IP**—The wizard increments the host portion of the last IP address in the static IP pool. Click **Apply**.
- **Same Last Digit**—The wizard adds the network portion of the IP address to the specified value. Type the host portion of the IP address and then click **Apply**.

The wizard updates the value in the **Additional IP addresses** column for each network. Verify the proposed IP addresses.

5. Click **Next**.
6. On the **Summary** page, review the information and then click **Finish**.

Perform a search

When the PowerProtect Search Engine is installed and configured, you can use the **File Search** functionality in the PowerProtect Data Manager UI to search across all indexed data to locate protected files and folders within virtual machine backup copies. When asset types are set up for index searching, the **File Search** button appears in the **Restore** menu for virtual machine assets.


Before performing a search, ensure that:

- A Search Engine node is set up.
- Search Indexing is enabled.

Virtual machine file level restore from a search

Within the **Restore** window of the PowerProtect Data Manager UI, **File Search** enables you to restore files from protected virtual machine backup copies to:

- The original virtual machine
- An alternate virtual machine.

 **NOTE:** Only file level virtual machine restore is available from **File Search**.

File level restore to original virtual machine using File Search

Use **File Search** in the PowerProtect Data Manager UI to restore files from multiple copies across one or more virtual machines to the same location on the original vCenter Server. Only the Administrator and the Restore Administrator roles can restore data.

Prerequisites

- Review the section [Supported platform versions for file-level restore](#) for supported platform and operating system versions.
- Review the section [File-level restore and SQL restore limitations](#) on page 247.

 **NOTE:** For file level restores to the original machine:

- The files must be restored from a Windows backup to a Windows machine, or from a Linux backup to a Linux machine.
- Restoring files from multiple copies with identical file names and paths from the same asset is not supported. In this case, only a file level restore to the alternate virtual machine is available.

Steps

1. From the PowerProtect Data Manager UI, select **Restore > Assets**, and then select the **Virtual Machine** tab.
The **Restore** window displays all the virtual machines available for restore.
2. Click **File Search**, and then perform the following:
 - a. Select a virtual machine from the **VM Name** list.
 - b. Use the **File Name** and **File Type** fields to search for specific files, or specify a file size or folder path to perform the search.
The files that match the search criteria display in the **Results** pane.
 - c. In the **Results** pane, select the files that you want to restore, and then click **Add**.
The **Results** pane is collapsed, and the **Selected Files** pane updates to display the current file selections.
 - d. Repeat steps b through d to select files from other virtual machines and copies. When finished with your selections, click **Restore**.

The **VM File Restore** wizard appears, displaying the **Location** page.

3. On the **Location** page:
 - a. Select **Restore to Original Location**.
 - b. Optionally, select **Overwrite existing files with the same name** to replace files in the original location with the files being restored if the files have the same name.
 - c. If you selected files from multiple virtual machines, and these virtual machines share the same credentials, move the **Use one set of credentials for all VMs** slider to the right to avoid retyping the credentials for each virtual machine.
 - d. For one or more virtual machines, type the virtual machine **User Name** and **Password**, and then click **Verify** to validate the credentials.
 - If there are administrator-level credentials that are associated with the virtual assets or protection policy being restored, specify end-user credentials.
 - If there are no administrator-level credentials that are associated with the virtual assets or protection policy being restored, specify administrator credentials. These credentials are handled as end-user credentials.

You are not required to wait for validation to complete before clicking **Verify** for another set of virtual machine credentials.

When validated, the **FLR Agent** is installed automatically on the restore destination, if it is not already installed. The **FLR Agent** facilitates the mounting and unmounting of disks and the browsing of files in the destination virtual machine and the backup copy. In order to complete the automatic **FLR Agent** installation, on Windows virtual machines the user must be an administrator account, and on Linux virtual machines the user must be the root user account, or a user in the operating system's local sudousers list. The section [FLR Agent for virtual machine file level restore](#) on page 248 provides more information.

- e. Optionally, leave **Keep FLR Agent Installed** selected if you do not want to remove the **FLR Agent** on the destination virtual machines after the restore completes.
- f. Click **Next**.

The **Summary** page appears.


4. On the **Summary** page:
 - a. Review the information to ensure that the restore details are correct. You can click **Edit** next to certain rows to change the information.
 - b. Click **Restore** or **Finish**.
5. Go to the **Jobs** window to monitor the restore.
A batch file level restore job with multiple files appears as a job group, with a progress bar and start time. A separate job entry is created for each copy that is being restored from.

File level restore to alternate virtual machine using File Search

Use **File Search** in the PowerProtect Data Manager UI to restore files from multiple copies across one or more virtual machines to a new location on a new virtual machine. This restore can be performed to the primary vCenter (the location of the original virtual machine), or a secondary vCenter Server. Only the Administrator and the Restore Administrator roles can restore data.

Prerequisites

- Review the section [Supported platform versions for file-level restore](#) for supported platform and operating system versions.
- Review the section [File-level restore and SQL restore limitations](#) on page 247.

 **NOTE:** For file-level restores to an alternate virtual machine:

- You can only restore files from a Windows backup to a Windows machine, or from a Linux backup to a Linux machine.
- Restore of multiple files from different operating systems to the same target virtual machine is not supported. In this case, only a file level restore to the original virtual machine is available.

Steps

1. From the PowerProtect Data Manager UI, select **Restore > Assets**, and then select the **Virtual Machine** tab.
The **Restore** window displays all the virtual machines available for restore.
2. Click **File Search**, and then perform the following:
 - a. Select a vCenter from the **vCenter Name** list.
 - b. Select a virtual machine from the **VM Name** list.
 - c. Use the **File Name** and **File Type** fields to search for specific files, or specify a file size or folder path to perform the search.
The files that match the search criteria display in the **Results** pane.
 - d. In the **Results** pane, select the files that you want to restore, and then click **Add**.
The **Results** pane is collapsed, and the **Selected Files** pane updates to display the current file selections.
 - e. Repeat steps b through d to select files from other virtual machines and copies. When finished with your selections, click **Restore**.
The **VM File Restore** wizard appears, displaying the **Location** page.
3. On the **Location** page:
 - a. Select **Restore to Alternate Location**.
The table on the page updates to display the available destination virtual machines within the vCenter and, when a specific virtual machine is selected, its location.
 - b. Expand the vCenter to locate the virtual machine that you want to restore to, and then select the virtual machine.
A prompt appears, requesting the credentials of this virtual machine.
 - c. Type the virtual machine **User Name** and **Password**, and then click **Verify** to validate the credentials.
When validated, the **FLR Agent** is installed automatically on the restore destination, if it is not already installed. The **FLR Agent** facilitates the mounting and unmounting of disks and the browsing of files in the destination virtual machine and the backup copy. In order to complete the automatic **FLR Agent** installation, on Windows virtual machines the user must be an administrator account, and on Linux virtual machines the user must be the root user account, or a user in the operating system's local sudousers list. The section [FLR Agent for virtual machine file level restore](#) on page 248 provides more information.
 - d. Optionally, leave **Keep FLR Agent Installed** selected if you do not want to remove the **FLR Agent** on the destination virtual machines after the restore completes.
 - e. When validation completes, click **Close** to return to the **Location** page.
The **Location** page updates with the available destination folders on the selected virtual machine.
 - f. Browse to the destination folder, or select a location and click **Add Folder** to create a destination within this folder.
 - g. Optionally, select **Overwrite existing files with the same name** to replace files in the destination folder with the files being restored if the files have the same name.
 - h. Click **Next**.
The **Summary** page appears.
4. On the **Summary** page:
 - a. Review the information to ensure that the restore details are correct. You can click **Edit** next to certain rows to change the information. If you are not restoring to the original virtual machine, an additional field appears for the **Target VM**.
 - b. Click **Restore** or **Finish**.
5. Go to the **Jobs** window to monitor the restore.
A batch file level restore job with multiple files appears as a job group, with a progress bar and start time. A separate job entry is created for each copy that is being restored from.

Troubleshooting Search Engine issues

This section lists troubleshooting and Search Engine issues.

Error displays during node failure

The following error might display during a search when a node fails:

Not able to deploy search-node.com. Another session "<host_name>" is already configured with the same hostname. Would you like to redeploy search node or delete the node?

If this error occurs, delete the node, and then retry the operation. If you choose to edit, delete the node and the new mode modal appears with your previous input. The input that caused the error is marked as critical.

Certificate issues

Issues with indexing backups and/or performing search queries might result when certificates that were deployed on the search node were corrupted.

Perform one of the following tests to determine certificate issues:

- Use the log bundle download utility in PowerProtect Data Manager to examine the Backup VM logs in VM Direct, and look for a log entry like the following:

```
ERROR: Failed to Upload File: /opt/emc/vproxy/runtime/tmp/vproxyd/
plugin/search/e6c356a1-fbaf-4231-9f6f-a0166b74909a/<search
node>-e081fdea-3599-4a6c-abc4-1b5487cb9a32-e523a94c-2d01-5234-ab3c-
7771cfab3c58-7f16bcbb72d7b49ea073356f0d7388ac08461827.db.zip to
https://<search node>:14251/upload, Error sending data chunk. Post
https://<search node>:14251/upload: x509: certificate signed by unknown authority
(possibly because of "crypto/rsa: verification error" while trying to verify
candidate authority certificate "PPDM Root CA ID-d5ec56b8-69ec-4183-9c94-7c0230408765"
```

- Examine the rest-engine logs in the search node (/opt/emc/search/logs/rest-engine/*.log), and look for certificate verification errors.
- Run a search either through the UI or through the API <PowerProtect Data Manager>/api/v2/file-instances and look for a certification verification error.

Examine the certificate files in the node(s) to investigate further. If necessary, regenerate the certificate files.

Access the Search Node to discover passwords

Use the following steps to discover the admin and root passwords for all deployed search nodes:

1. Connect to the PowerProtect Data Manager console and change to the root user.
2. Change directory to /opt/emc/vmdirect.
3. Source unit/vmdirect.env.
4. Run bin/infranodemgmt get -secret.

Verify certificates

Use this procedure to verify that certificates are valid and uncorrupted:

1. Verify that the rootca.pem file is the same in all the relevant nodes (search node, PowerProtect Data Manager, and VM Direct node).

NOTE: The rootca.pem file name is different on each node:

- PowerProtect Data Manager— /etc/ssl/certificates/rootca/rootca.pem
- Search node— /var/lib/dellemc/vmboot/trust/thumbprint
- VM Direct— /var/lib/dellemc/vmboot/trust/thumbprint

2. Run the following openssl command to find out whether the root certificate file is corrupt or invalid: `openssl verify <rootca.pem>`

Response:

```
/var/lib/dellemc/vmboot/trust/thumbprint: C = US,
O = DELL Corporation,
CN = PPDM Root CA ID-4c9de850-24ab-42ec-a9a7-6080849d0d24

error 18 at 0 depth lookup:self signed certificate
```

OK

Ensure that the CN values match.

Certificate verification fails

If the certificate verification steps fail, you must re-create the certificates on the Search Node or VM Direct node:

1. Connect to the PowerProtect Data Manager console and change to the root user.
2. Use the `Get` command in the `infranodemgmt` utility to determine the search node FQDN.
3. Run `/usr/local/brs/puppet/scripts/generate_certificates.sh -n -c -b <search node FQDN>`
A properties file is created in the `/root` directory called `<search node FQDN>.properties`.
4. Open this file to determine the location of the generated certificates. They should be located in `/etc/ssl/certificates/<search node FQDN>`.
5. From a separate terminal, SSH into the search node using the password that was revealed with the `infranodemgmt Get` call in step 2.
6. Change directory to `/var/lib/dellemc/vmboot/trust` and move the `key`, `cert`, and `thumbprint` files over.
7. Copy the certificate files that were generated in PowerProtect Data Manager as follows:
 - `otca.pem` to `thumbprint`
 - `<search node FQDN>key.pem` to `key`
 - `<search node FQDN>.pem` to `cert`
8. Paste the files to `/var/lib/dellemc/vmboot/trust`.
9. Set the permissions for the `key`, `cert`, and `thumbprint` files to **0644**, and then set the ownership of these files to **root:app**
10. Restart the rest-engine daemon or the vproxyd daemon) to pick up the new certificates: `systemctl restart search-rest-engine`.
11. Check the rest-engine log file (`/opt/emc/search/logs/rest-engine/rest-engine-daemon-<fqdn>.log`) to verify that the service started successfully.

Ensure that the following message appears:

A valid Root CA certificate of backup server was provided during deployment

Result: Backup with indexing executes successfully and search service is functional.

Search cluster is full


If the search cluster is full, you can deploy additional nodes by following the steps in [Set up and manage indexing](#) on page 46.

If the search cluster runs out of space and you do not want to deploy an additional node, you have the following options:

- Disable the service
- Shorten the expiration time to remove indexes sooner
- Remove indexes manually


To disable the service, complete the following steps:

1. From the PowerProtect Data Manager UI, select **Infrastructure > Search Engine**.
2. Select the cluster, and then click **Configure Cluster**.
3. In the **Configure Search Cluster** dialog box, switch the **Search Indexing** button to turn it off, and then click **Save**.

 **NOTE:** This setting applies to all indexes in all protection policies in the Search Cluster.

To shorten the expiration time to remove indexes sooner, complete the following steps:

1. From the PowerProtect Data Manager UI, select **Infrastructure > Search Engine**.
2. Select the cluster, and then click **Configure Cluster**.
3. In the **Configure Search Cluster** dialog box, modify the **Search Index Expiration** and click **Save**. A recommended formula to determine the expiration time is: Delete Index when Today = Backup-Date + Expiration Days + 1 day. That is, one day after the backup expires.

 **NOTE:** This setting applies to all indexes in all protection policies in the Search Cluster.

To remove indexes manually, complete the following steps:

1. Use SSH to log in to the Search virtual machine.
2. Create a snapshot of the Search cluster using the following format:

```
{
  Command:  "APP_SNAPSHOT",
  Title:    "Initiate Index/Search Cluster Snapshot Process",
  AsyncCmd: false,
  Properties: {
    "Name": {
      Description: "Used to uniquely identify a particular snapshot",
      Type:        STRING
    },
    "Action": {
      Description: "Action to perform, 'Create', 'Delete', 'Restore' or
'Cancel' a Snapshot",
      Type:        STRING
    },
    "NFSTHost": {
      Description: "NFS Host serving snapshot backup area.",
      Type:        STRING
    },
    "NFSExport": {
      Description: "NFS Export path to mount too.",
      Type:        STRING
    },
    "NFSDirPath": {
      Description: "NFS directory path to write too.",
      Type:        STRING
    }
  }
}
```

For example:

```
{
  "Command": "APP_SNAPSHOT",
  "Title": "",
  "AsyncCmd": false,
  "Properties": {
    "Action": {
      "Description": "",
      "Required": false,
      "Type": "string",
      "IsArray": false,
      "Value": "Create",
      "Default": null
    },
    "Name": {
      "Description": "",
      "Required": false,
      "Type": "string",
      "IsArray": false,
      "Value": "DataManager_Catalog_Cluster_snapshot_2019-10-16-12-57-16",
      "Default": null
    },
    "NFSTHost": {
      "Value": "10.25.87.88"
    },
    "NFSExport": {
      "Value": "/mnt/shared"
    },
    "NFSDirPath": {
      "Value": ""
    }
  }
}
```

3. You can delete indexes by protection policy or by asset. If the JSON command is stored at /home/admin/remove-plc.json, run the command, ./searchmgmt -I /home/admin/remove-plc.json.

- Use the following format to delete indexes by protection policy:

```
{
    "Command": "APP_REMOVE_ITEMS",
    "AsyncCmd": false,
    "Properties": {
        "Action": {
            "Description": "Action to perform,
'AssetDelete', 'PLCDelete'",
            "Required": true,
            "Value": "PLCDelete",
        },
        "PLCID": {
            "Description": "PLC ID of item(s) to delete.",
            "Required": true,
            "Value": "7676d753-b57e-a572-6daf-33689933456d",
        }
    }
}
```

- Use the following format to delete indexes by asset type:

```
{
    "Command": "APP_REMOVE_ITEMS",
    "AsyncCmd": false,
    "Properties": {
        "Action": {
            "Description": "Action to perform,
'AssetDelete', 'PLCDelete'",
            "Required": true,
            "Value": "AssetDelete",
        },
        "AssetID": {
            "Description": "Optional, Asset ID of item(s)
to delete.",
            "Required": false,
            "Value": "503dd753-b57e-a572-6daf-44680033755f",
        },
        "PLCID": {
            "Description": "PLC ID of item(s) to delete.",
            "Required": true,
            "Value": "7676d753-b57e-a572-6daf-33689933456d",
        }
    }
}
```

NOTE:

- The time to complete the execution of these procedures depends on the number of backup copy asset indexes being deleted.
- This procedure does not impact regular operation of the cluster.

Troubleshooting a locked Search Engine Node

The nodes on the PowerProtect Data Manager Search cluster are configured with IP addresses that can be accessed externally. These nodes are configured with admin or root user accounts, which are only used to log in to the Search nodes for troubleshooting software issues. The password management policies for these accounts are set to lock the admin user account if there are three wrong password attempts within a 5 minute time period. If you try to access the node while the admin user account is locked, the amount of time that the account remains locked increases.

There is no public interface available that enables you to access the search node by using admin credentials. All required information about the Search Engine nodes is obtained through the PowerProtect Data Manager UI.

A Search node might become locked for the following reasons:

- A user or program tries to SSH into the search node and makes three wrong attempts at entering the password.
- Running monitoring software that tries to log in to the Search node with the wrong admin credentials and locks the system.
- Running Penetration Testing (PEN) on the VMs in the vCenter.

The Search admin user account enables the PowerProtect Data Manager system to perform different operations on the Search node, such as obtaining the health status of the node. If the account is locked, the health status of the node is reported as "Failed." When one of the nodes in the Search cluster is in a failed state, the entire Search cluster becomes unavailable. As a result, the Search cluster is unable to perform any indexing or search operations.

Workaround

To work around this issue, first access the Search node to discover the admin and root credentials for the node. After you discover the node credentials, log in to the node through the vCenter console to reset the admin credentials.

Use the following steps to discover the admin and root passwords for all deployed Search nodes:

1. Connect to the PowerProtect Data Manager console and change to the root user.
2. Change directory to `/opt/emc/vmdirect`
3. Run `unit/vmdirect.env`
4. Run `bin/infranodemgmt get -secret`

Before you access the Search node through the vCenter console, determine why the admin account is locked.

Use the following steps to unlock the admin user account:

1. Log in to the vCenter where the Search node is present.
2. Select the Search node from the **VMs and Templates** view in the left pane of the vSphere Client home page.
3. Launch a PowerProtect Data Manager VM vCenter console.
4. Log in to the vCenter console with the root username and password.
5. Run the following command to reset the admin user account credentials:

```
/sbin/pam_tally2 --user admin --reset
```

Managing Assets

Topics:

- [About asset sources, assets, and storage](#)
- [Prerequisites for discovering asset sources](#)
- [Enable an asset source](#)
- [Delete an asset source](#)
- [Adding a vCenter Server asset source](#)
- [VM Direct protection engine overview](#)
- [Adding a Cloud Snapshot Manager tenant](#)

About asset sources, assets, and storage

In PowerProtect Data Manager, assets are the basic units that PowerProtect Data Manager protects. Asset sources are the mechanism that PowerProtect Data Manager uses to manage assets and communicate with the protection storage where backup copies of the assets are stored.

PowerProtect Data Manager supports Dell EMC PowerProtect DD Management Center (DDMC) as the storage and programmatic interface for controlling protection storage systems.

Asset sources can be a vCenter Server, Kubernetes cluster, application host, SMIS server, or Cloud Snapshot Manager tenant. Assets can be virtual machines, Exchange databases, SQL databases, Oracle databases, SAP HANA databases, file systems, Kubernetes namespaces, or storage groups.

Before you can add an asset source, you must enable the source within the PowerProtect Data Manager UI.

About vCenter Server asset sources and virtual assets

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


The virtual assets for the vCenter Server appear in the **Assets** window of the PowerProtect Data Manager UI under the **Virtual Machine** tab.

The initial vCenter Server discovery identifies all ESXi clusters, hosts, and virtual machines within the vCenter Server. Subsequent discoveries can be performed 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. Dell EMC recommends 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 creating and applying protection rules to determine which assets are included in a protection policy based on rule definitions.

About other asset sources

In addition to vCenter Server asset sources, PowerProtect Data Manager provides the option to enable the following asset sources to protect other asset types.

 **NOTE:** The *PowerProtect Data Manager Administration and User Guide* does not provide instructions for Kubernetes clusters or agent asset source management. Refer to the PowerProtect Data Manager online help or individual Kubernetes and agent user guides for more information.

File System agent

After the File System agent is approved and registered in the PowerProtect Data Manager UI, PowerProtect Data Manager integrates with the agent to enable an application administrator to protect and recover data on the File System host, and to check and monitor backup compliance against protection policies.

Kubernetes cluster

After the Kubernetes cluster asset source is added and registered in the PowerProtect Data Manager UI, PowerProtect Data Manager enables protection of PVCs and namespace data on the Kubernetes or Tanzu Kubernetes cluster.

NAS agent

After the NAS asset source is added and registered in the PowerProtect Data Manager UI, PowerProtect Data Manager enables protection of NAS assets.

Microsoft Exchange agent

After the Microsoft Exchange agent is approved and registered in the PowerProtect Data Manager UI, PowerProtect Data Manager integrates with the agent to enable an application administrator to protect and recover the Exchange application data on the application host, and to check and monitor backup compliance against protection policies.

Microsoft SQL agent

After the Microsoft SQL agent is approved and registered in the PowerProtect Data Manager UI, PowerProtect Data Manager integrates with the agent to enable an application administrator to protect and recover the SQL application data on the application host, and to check and monitor backup compliance against protection policies.

Oracle RMAN agent

After the Oracle RMAN agent is approved and registered in the PowerProtect Data Manager UI, PowerProtect Data Manager integrates with the agent to enable an application administrator to protect and recover the Oracle application data on the application host, and to check and monitor backup compliance against protection policies.

SAP HANA agent

After the SAP HANA agent is approved and registered in the PowerProtect Data Manager UI, PowerProtect Data Manager integrates with the agent to enable an application administrator to protect and recover the SAP HANA application data on the application host, and to check and monitor backup compliance against protection policies.

Storage Direct agent for Storage Data Management

Storage Data Management uses snapshot backup technology to protect data on VMAX and PowerMax storage arrays by moving storage group data from the array to a DD system. After the Storage Direct agent is approved and registered in the PowerProtect Data Manager UI, and the DD system and the SMIS server are added and discovered, the Storage Direct agent enables you to discover the storage groups in the storage arrays, and assign unprotected storage groups to a protection policy for backup and recovery operations.

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 guides provide information.
- Log in as a user with the Administrator role. Only the Administrator role can manage asset sources.

- For a new system, enable one or more asset sources for the types of assets that you want to protect. [Enable an asset source](#) on page 60 provides more information.
- Configure all asset sources with an NTP server.
- Before you register an SQL application, ensure that the DD system has been discovered successfully.
- For discovery of Application Agent and 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.
- Discovery of a vCenter Server asset source will exclude the following:
 - Virtual machines with a status of **Inaccessible**, **Invalid**, or **Orphaned**.
 - The virtual machine template
 - The shadow (or standby) virtual machine created by Dell EMC RecoverPoint for Virtual Machines, also referred to as the vRPA copy.

Prior to performing the vCenter discovery, verify the status of any virtual machines that you want to discover.

Enable an asset source

An asset source, such as a vCenter Server, must be enabled in PowerProtect Data Manager before you can add and register the asset source for the protection of assets.

About this task

Only the Administrator role can manage asset sources.

There are some circumstances where enabling an asset source is not required, such as the following:

- For application agents and other agents such as File System and Storage Direct, an asset source is enabled automatically when you register and approve the agent host. For example, if you have not enabled an Oracle asset source but have registered the application host through the API or the PowerProtect Data Manager UI, PowerProtect Data Manager automatically enables the Oracle asset source.
- When you update to the latest version of PowerProtect Data Manager from an earlier release, any asset sources that were previously enabled appear in the PowerProtect Data Manager UI. On a new installation, however, no asset sources are enabled by default.

Steps

1. From the PowerProtect Data Manager UI, select **Infrastructure > Asset Sources**, and then click **+** to reveal the **New Asset Source** tab.
2. In the pane for the asset source that you want to add, click **Enable Source**.
The **Asset Sources** window updates to display a tab for the new asset source.

Results

You can now add or approve the asset source for use in PowerProtect Data Manager. For a vCenter Server, Kubernetes cluster, SMIS Server, or PowerProtect Cloud Snapshot Manager tenant, select the appropriate tab in this window and click **Add**. For an application agent, select **Infrastructure > Application Agents** and click **Add** or **Approve** as required.

i NOTE: Although you can add a Cloud Snapshot Manager tenant to PowerProtect Data Manager in order to view its health, alerts, and the status of its protection, recovery, and system jobs, you cannot manage the protection of its assets from PowerProtect Data Manager. To manage the protection of its assets, use Cloud Snapshot Manager. For more information, see the *PowerProtect Cloud Snapshot Manager Online Help*.

Disable an asset source

If you enabled an asset source that you no longer require, and the host has not been registered in PowerProtect Data Manager, perform the following steps to disable the asset source.

About this task

NOTE: An asset source cannot be disabled when one or more sources are still registered or there are backup copies of the source assets. For example, if you registered a vCenter Server and created policy backups for the vCenter virtual machines, then you cannot disable the vCenter asset source. But if you register a vCenter Server and then delete the vCenter without creating any backups, you can disable the asset source.

Steps

1. From the PowerProtect Data Manager UI, select **Infrastructure > Asset Sources**, and then select the tab of the asset source that you want to disable.
If no host registration is detected, a red **Disable** button appears.
2. Click **Disable**.

Results

PowerProtect Data Manager removes the tab for this asset source.

Delete an asset source

If you want to remove an asset source that you no longer require, perform the following steps to delete the asset source in the PowerProtect Data Manager UI.

About this task

Only the Administrator role can manage the asset sources.

Steps

1. From the PowerProtect Data Manager UI, select **Infrastructure > Asset Sources**, and then select the tab for the type of asset source that you want to delete.
2. Select the asset source name in the asset source list, and then click **Delete**.
3. At the warning prompt that appears, click **Continue**.
The asset source is deleted from the list.

Results

PowerProtect Data Manager removes the specified asset source in the **Asset Sources** window.

For all asset sources except the vCenter Server, any associated assets that are protected by the protection policy are removed from the protection policy and their status is changed to deleted. These assets can be deleted automatically or manually. The *PowerProtect Data Manager Administration and User Guide* provides details on how to remove assets from PowerProtect Data Manager.

The copies of assets from the asset source are retained (not deleted). You can delete the copies from the copies page, if required.

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.

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 for virtual machine protection and Tanzu Kubernetes guest cluster protection.

Prerequisites

- Ensure that the asset source is enabled. [Enable an asset source](#) on page 60 provides instructions.
- Log in as a user with the Administrator role. Only the Administrator role can manage asset sources.
- By default, PowerProtect Data Manager enforces SSL certificates during communication with vCenter Server. If a certificate appears and you trust the certificate, click **Verify**.

Note, however, that SSL certificate enforcement requires that the common name (cn) of the x509 certificate on the vCenter Server matches the hostname of the vCenter URL. The common name of the x509 certificate is typically the vCenter server fully qualified domain name (FQDN), but it could be the vCenter server IP address. You can inspect the vCenter server SSL certificate to determine whether the x509 common name is an FQDN or IP. When creating an asset source resource, in order to pass SSL certificate enforcement, the asset source resource hostname must match the common name of the x509 certificate on the vCenter server.

 **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 vCenter SSL certificate validation](#) on page 246.

Steps

1. From the left navigation pane, 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 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.

 **NOTE:** For a vCenter Server, it is recommended 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**.

 **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 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**.

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


7. By default, the vCenter discovery occurs automatically after adding the vCenter, and subsequent discoveries are incremental. If you want to schedule a full discovery at a certain time every day, move the **Schedule Discovery** slider to the right, and then specify a time.
8. If there is no hosting vCenter and you want to make this the vCenter Server that hosts PowerProtect Data Manager, select **Add as hosting vCenter**. If a vCenter Server has already been added as the hosting vCenter, this option will be greyed out. [Specify a vCenter Server as the PowerProtect Data Manager host](#) on page 157 provides more information about adding a host vCenter.
9. If the vCenter server SSL certificate cannot be trusted automatically, a dialog box appears requesting certificate approval. Review the certificate, and then click **Verify**.
10. Click **Save**.

The vCenter Server information that you entered now appears as an entry in a table on the **Asset Sources** window. You can click the magnifying glass icon next to the entry to view more details, such as the next scheduled discovery, the number of assets within the vCenter, and whether the **vSphere Plugin** is enabled.

 **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 discovery, PowerProtect Data Manager starts an incremental discovery in the background periodically to keep updating PowerProtect Data Manager with vCenter changes. You can always do an on-demand discovery.

11. Optionally, you can set warning and failure thresholds for the available space on the datastore. Setting these thresholds enables you to check if enough storage space is available in the datastore to save the snapshot of the virtual machine during the backup process. The backup completes with a warning in the logs if the available free space in the datastore is less than or equal to the percentage indicated in the **Datastore Free Space Warning Threshold**. The backup fails if the available free space in the datastore is less than or equal to the percentage indicated in the **Datastore Free Space Failure Threshold**. To add Datastore Free Space Warning and Failure Thresholds:
 - a. Click the gear icon to open the **vCenter Settings** dialog.
 - b. Type a percentage value to indicate when a warning message should display due to low datastore free space.
 - c. Type a percentage value to indicate when a virtual machine backup failure should occur due to low datastore free space.
 - d. Click **Save**.

 **NOTE:** Datastore free space thresholds are disabled by default.

12. Select **Infrastructure > Assets**.


The **Assets** window appears.

13. If not already selected, click the **Virtual Machine** tab.

Results

Upon a successful discovery of the vCenter server asset source, the virtual machine assets in the vCenter display in the **Infrastructure > Assets** window.

You can modify the details for the vCenter asset source by selecting the vCenter in the **Infrastructure > Asset Sources** window and clicking **Edit**. You cannot, however, clear the **Add as hosting vCenter** checkbox when editing an asset source if this vCenter Server has already been added as the hosting vCenter. For this operation, use the **Hosting vCenter** window, as described in the section [Specify a vCenter Server as the PowerProtect Data Manager host](#) on page 157.

 **NOTE:** Discovery time is based on networking bandwidth. The resources that are discovered and the resources that are performing the discovery impact performance each time that you initiate a discovery process. It might appear that PowerProtect Data Manager is not updating the Asset Sources data while the discovery is in progress.

Next steps

Add a VM Direct appliance to facilitate data movement, and then create virtual machine protection policies to back up these assets. The PowerProtect Data Manager software comes 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 be deployed since the embedded VM Direct engine has limited capacity for performing backup streams. To add a VM Direct Engine, select **Infrastructure > Protection Engines**.

Creating a dedicated vCenter user account

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” could 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 a vCenter user account when you add the vCenter as an asset source in the UI. When you add the vCenter, ensure that you specify a user whose role is defined at the vCenter level and not 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.

NOTE: For the privileges required when administering PowerProtect Data Manager in a cloud environment, see [Specify the required privileges for a dedicated cloud-based vCenter user account](#) on page 193. For the additional privileges required when using the Transparent Snapshot Data Mover (TSDM) protection mechanism for virtual machine crash-consistent data protection, see [Additional privileges required for a dedicated vCenter user account to use Transparent Snapshot Data Mover](#) on page 178.

Table 25. Minimum required vCenter user account privileges

Setting	vCenter 6.5 and later required privileges	PowerCLI equivalent required privileges
Alarms	<ul style="list-style-type: none"> Create alarm Modify alarm 	<pre>\$privileges = @('System.Anonymous', 'System.View', 'System.Read', 'Alarm.Create', 'Alarm.Edit', 'Cryptographer.AddDisk', 'Cryptographer.Access', 'Cryptographer.RegisterVM', 'Datastore.Rename', 'Datastore.Move', 'Datastore.Delete', 'Datastore.Browse', 'Datastore.DeleteFile', 'Datastore.FileManagement', 'Datastore.AllocateSpace', 'Datastore.Config', 'Extension.Register', 'Extension.Unregister', 'Extension.Update', 'Folder.Create', 'Global.ManageCustomFields', 'Global.SetCustomField', 'Global.LogEvent', 'Global.CancelTask', 'Global.Licenses', 'Global.Settings', 'Global.DisableMethods', 'Global.EnableMethods', 'Host.Config.Storage', 'InventoryService.Tagging.AttachTag', 'InventoryService.Tagging.ObjectAttachable', 'InventoryService.Tagging.CreateTag', 'InventoryService.Tagging.CreateCategory', 'Network.Config', 'Network.Assign', 'Resource.AssignVMToPool', 'Resource.HotMigrate', 'Resource.ColdMigrate', 'Sessions.ValidateSession', 'StorageProfile.Update', 'StorageProfile.View', 'Task.Create', 'Task.Update', 'VApp.ApplicationConfig', 'VApp.Export', 'VApp.Import', 'VirtualMachine.Config.Rename', 'VirtualMachine.Config.Annotation', 'VirtualMachine.Config.AddExistingDisk'</pre>
Cryptographic operations	<ul style="list-style-type: none"> Add disk Direct Access Register VM 	
Datastore	<ul style="list-style-type: none"> Allocate space Browse datastore Configure datastore Low level file operations Move datastore Remove datastore Remove file Rename datastore 	
Extension	<ul style="list-style-type: none"> Register extension Unregister extension Update extension 	
Folder	<ul style="list-style-type: none"> Create folder 	
Global	<ul style="list-style-type: none"> Cancel task Disable methods Enable methods Licenses Log event Manage custom attributes Set custom attribute Settings 	
Host	<ul style="list-style-type: none"> Configuration > Storage partition configuration 	
vSphere Tagging	<ul style="list-style-type: none"> Assign or Unassign vSphere Tag Assign or Unassign vSphere Tag on Object NOTE: This only applies to vCenter 7.0 and later. Create vSphere Tag Create vSphere Tag Category 	
Network	<ul style="list-style-type: none"> Assign network Configure 	
Resource	<ul style="list-style-type: none"> Assign virtual machine to resource pool Migrate powered off virtual machine Migrate powered on virtual machine 	

Table 25. Minimum required vCenter user account privileges (continued)

Setting	vCenter 6.5 and later required privileges	PowerCLI equivalent required privileges
Sessions	<ul style="list-style-type: none">Validate session	<pre>, '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.GuestOperations.Query', 'VirtualMachine.GuestOperations.Modify' , 'VirtualMachine.GuestOperations.Execute' , '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.Inventory.Create', 'VirtualMachine.Inventory.Register', 'VirtualMachine.Inventory.Delete', 'VirtualMachine.Inventory.Unregister', 'VirtualMachine.Provisioning.DiskRandomAccess', 'VirtualMachine.Provisioning.DiskRandomRead', 'VirtualMachine.Provisioning.GetVmFiles', 'VirtualMachine.Provisioning.MarkAsTemplate', 'VirtualMachine.State.CreateSnapshot', 'VirtualMachine.State.RevertToSnapshot' , 'VirtualMachine.State.RemoveSnapshot',) New-VIRole -Name 'PowerProtect' -Privilege (Get-VIPrivilege -Id \$privileges)</pre>
SPBM policy restore	<ul style="list-style-type: none">Profile-driven storageProfile-driven storage updateProfile-driven storage view	
Tasks	<ul style="list-style-type: none">Create taskUpdate task	
vApp	<ul style="list-style-type: none">ExportImportvApp application configuration	
Virtual Machine		
Change Configuration	<ul style="list-style-type: none">Acquire disk leaseAdd existing diskAdd new diskAdd or remove deviceAdvanced configurationChange CPU countChange MemoryChange SettingsChange Swapfile placementChange resourceConfigure Host USB deviceConfigure Raw deviceConfigure managedbyExtend virtual diskModify device settingsReload from pathRemove diskRenameReset guest informationSet annotationToggle disk change trackingUpgrade virtual machine compatibility	
Edit Inventory	<ul style="list-style-type: none">Create newRegisterRemoveUnregister	
Guest operations	<ul style="list-style-type: none">Guest operation modificationsGuest operation program executionGuest operation queries	
Interaction	<ul style="list-style-type: none">Configure CD mediaConnect devicesConsole interactionGuest operating system management by VIX APIInstall VMware ToolsPower offPower onReset	
Provisioning	<ul style="list-style-type: none">Allow disk access	

Table 25. Minimum required vCenter user account privileges (continued)

Setting	vCenter 6.5 and later required privileges	PowerCLI equivalent required privileges
	<ul style="list-style-type: none"> Allow read-only disk access Allow virtual machine download Mark as template 	
Snapshot Management	<ul style="list-style-type: none"> Create snapshot Remove snapshot Revert to snapshot 	

VM Direct protection engine overview

The VM Direct protection engine provides two functions within PowerProtect Data Manager:

- A virtual machine data protection solution—Deploy a VM Direct Engine in the vSphere environment to perform virtual machine snapshot backups, which improves performance and reduces network bandwidth utilization by using the protection storage source-side deduplication.
- A Tanzu Kubernetes guest cluster data protection solution—Deploy a VM Direct Engine in the vSphere environment for protection of vSphere CSI-based persistent volumes, for which it is required to use a VM Proxy instead of the cProxy, for the management and transfer of backup data.

The VM Direct protection engine is enabled after you add a vCenter Server in the **Asset Sources** window, and allows you to collect VMware entity information from the vCenter Server and save VMware virtual machines and Tanzu Kubernetes guest cluster namespaces and PVCs 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 appliances, and add an external VM Direct appliance to facilitate data movement, select **Infrastructure > Protection Engines**. [Add a VM Direct Engine](#) on page 66 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 appliance, the **VM Direct Engines** pane provides the following information:

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

Requirements for an external VM Direct Engine

When adding an external VM Direct Engine, note the following system requirements:

- CPU: 4 * 2 GHz (4 virtual sockets, 1 core for each socket)
- Memory: 8 GB RAM
- Disks: 2 disks (59 GB and 98 GB)
- Internet Protocol: IPv4 only
- SCSI controller: maximum of 4
- NIC: One vmxnet3 NIC with one port

Add a VM Direct Engine

Perform the following steps in the **Protection Engines** window of the PowerProtect Data Manager UI to deploy an external VM Direct Engine, also referred to as a VM proxy. The VM Direct engine facilitates data movement for virtual machine

protection policies, Kubernetes cluster protection policies that require a VM proxy instead of the cProxy, and network attached storage (NAS) protection policies.

Prerequisites

Review the sections [Requirements for an external VM Direct Engine](#) on page 66 and [Transport mode considerations](#) on page 252.


If applicable, complete all of the virtual network configuration tasks before you assign any virtual networks.

About this task


The PowerProtect Data Manager software comes 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. Dell Technologies recommends that you deploy external proxies by adding a VM Direct Engine for the following reasons:

- An external VM Direct Engine for VM proxy backup and recovery can provide improved performance and reduce network bandwidth utilization by using source-side deduplication.
- The embedded VM Direct engine has limited capacity for backup streams.
- The embedded VM Direct engine is not supported for VMware Cloud on AWS operations.

An external VM Direct engine is not required for virtual machine protection policies that use the Transparent Snapshot Data Mover (TSDM) protection mechanism. For these policies, the embedded VM Direct engine is sufficient.

 **NOTE:** Cloud-based OVA deployments of PowerProtect Data Manager do not support the configuration of data-traffic routing or VLANs. Those deployments skip the **Networks Configuration** page.

Steps

1. From the left navigation pane, select **Infrastructure > Protection Engines**.
The **Protection Engines** window appears.
2. In the **VM Direct Engines** pane of the **Protection Engines** window, click **Add**.
The **Add Protection Engine** wizard displays.
3. On the **Protection Engine Configuration** page, complete the required fields, which are marked with an asterisk.
 - **Hostname, Gateway, IP Address, Netmask, and Primary DNS**—Note that only IPv4 addresses are supported.
 - **vCenter to Deploy**—If you have added multiple vCenter Server instances, select the vCenter on which to deploy the protection engine.
 **NOTE:** Ensure that you do not select the internal vCenter Server.
 - **ESX Host/Cluster**—Select on which cluster or ESXi host you want to deploy the protection engine.
 - **Network**—Displays all the networks that are available under the selected ESXi Host/Cluster. For virtual networks (VLANs), this network carries management traffic.
 - **Data Store**—Displays all datastores that are accessible to the selected ESXi Host/Cluster based on ranking (whether the datastores are shared or local), 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 protection engine resides, or leave the default selection of **<automatic>** to allow PowerProtect Data Manager to determine the best location to host the protection engine.
 - **Transport Mode**—Select **Hot Add**.
 - **Supported Protection Type**—Select whether this protection engine is intended for **Virtual Machine, Kubernetes** Tanzu guest cluster, or **NAS** asset protection.
4. Click **Next**.
5. On the **Networks Configuration** page:

If this is a cloud-based OVA deployment of PowerProtect Data Manager, click **Next** and proceed to step 7.

The **Networks Configuration** page configures the virtual network (VLAN) to use for backup data. To continue without virtual network configuration, leave the **Preferred Network Portgroup** selection blank and then click **Next**.

- a. From the **Preferred Network Portgroup** list, select a VST (Virtual Switch Tagging) or VGT (Virtual Guest Tagging) network.
If you select a VGT portgroup, the list displays all virtual networks within the trunk range. If you select a VST portgroup, the list displays only the virtual network for the current VLAN ID.
- b. Select one or more virtual networks from the list.

A protection engine requires an IP address from the static IP pool for each selected virtual network. If there are not enough IP addresses in a pool, the wizard prompts you to supply additional addresses for that network.

- c. If required, type an available static IP address or IP address range in the **Additional IP Addresses** column for the indicated virtual network.

For convenience when working with multiple virtual networks, you can also use one of the **Auto Expand** options:

- **Expand Last IP**—The wizard increments the host portion of the last IP address in the static IP pool. Click **Apply**.
- **Same Last Digit**—The wizard adds the network portion of the IP address to the specified value. Type the host portion of the IP address and then click **Apply**.

The wizard updates the value in the **Additional IP addresses** column for each selected network. Verify the proposed IP addresses.

- d. Click **Next**.

6. When adding a VM Direct engine for Kubernetes guest cluster protection, add a second network interface card (NIC) if the PowerProtect controller pod running in the guest cluster cannot reach the vProxy on the primary network. Provide information for the second NIC, and then click **Next**.

7. On the **Summary** page, review the information and then click **Finish**.

The protection engine is added to the **VM Direct Engines** pane. An additional column indicates the engine purpose. Note that it can take several minutes to register the new protection engine in PowerProtect Data Manager. The protection engine also appears in the **vSphere Client**.

Results

When an external VM Direct Engine is deployed and registered, PowerProtect Data Manager uses this engine instead of the embedded VM Direct engine for any data protection operations that involve virtual machine protection policies. If all external VM Direct Engines are unavailable, PowerProtect Data Manager uses the embedded VM Direct engine as a fallback to perform limited scale backups and restores. If you do not want to use the external VM Direct Engine, you can disable this engine.

[Additional VM Direct actions](#) on page 68 provides more information.

NOTE: The external VM Direct Engine is always required for VMware Cloud on AWS operations, Kubernetes cluster protection policies that require a VM Proxy instead of the cProxy, and NAS protection policies. If no external VM Direct Engine is available for these solutions, data protection operations fail.

Next steps

If the protection engine 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, delete the failed protection engine and then add the protection engine in the **Protection Engines** window.

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

Additional VM Direct actions


For additional VM Direct actions, such as enabling, disabling, redeploying, or deleting the VM Direct Engine, or changing the network configuration, use the **Protection Engines** window in the PowerProtect Data Manager UI. To throttle the capacity of VM Direct engines, use a command-line tool on PowerProtect Data Manager.

To get external VM Direct Engine credentials, see the procedure in the *PowerProtect Data Manager Security Configuration Guide*.

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 updated during a PowerProtect Data Manager update.

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. On the **Protection Engines** window, 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. On the **Protection Engines** window, 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 update 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 update of the VM Direct Engine did not occur due to network inaccessibility or an environment error, the **Redeploy** option enables you to manually update the VM Direct Engine to the version currently in use with the PowerProtect Data Manager software. Perform the following steps to manually redeploy the VM Direct Engine.

1. On the **Protection Engines** window, 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 **Redeploy** from the menu.

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

Update the DNS or gateway during redeployment

Optionally, if you want to update the vProxy DNS and/or gateway during the VM Direct Engine redeployment, you can use one of the following commands:

- To update both the gateway and DNS, run `./vproxymgmt redeploy -vproxy_id VM Direct Engine ID -updateDns DNS IPv4 address -updateGateway Gateway IPv4 address`
- To update the gateway only, run `./vproxymgmt redeploy -vproxy_id VM Direct Engine ID -updateGateway Gateway IPv4 address`
- To update DNS only, run `./vproxymgmt redeploy -vproxy_id VM Direct Engine ID -updateDns DNS IPv4 address`

Edit the network configuration for a VM Direct Engine

If VM Direct Engine deployment failed because of a virtual network configuration problem, you can update the configuration to add additional IP addresses to the static IP pool. You can also add the VM Direct Engine to a virtual network in the same VGT port group.

Perform the following steps to change the network configuration:

1. On the **Protection Engines** window, select the VM Direct Engine from the table in the **VM Direct Engines** pane.
2. Click **Edit**.
3. Select the row that corresponds to the virtual network with the configuration error, or the virtual network to which you want to add the VM Direct Engine.
4. Type an available static IP address or IP address range in the **Additional IP Addresses** column.
5. Click **Next**.
6. On the **Summary** page, verify the network settings, and then click **Next**.

To change other network configuration settings, delete the VM Direct Engine and then deploy a new VM Direct Engine.

Throttle capacity of a VM Direct Engine

In performance-limited environments, you can use a command-line tool on PowerProtect Data Manager to reduce the maximum capacity of VM Direct engines.

- The default value for *VM Configured Capacity Units* of an external VM Direct engine is 100. The minimum value is 4.
- A VM Direct engine can backup one disk with 4 units of capacity at a time.

Perform these steps to throttle the capacity of one or more VM Direct engines:

1. Connect to the PowerProtect Data Manager console and change to the root user.
2. Type: **source /opt/emc/vmdirect/unit/vmdirect.env**
3. To view the list of VM Direct engines and their IDs, type: **/opt/emc/vmdirect/bin/vproxymgmt get -list**
4. To change the capacity of a VM Direct engine, type (once per engine): **/opt/emc/vmdirect/bin/vproxymgmt modify -vproxy_id [VProxy ID] -capacity [percentage]**
5. To verify the change in *VM Configured Capacity Units*, type: **/opt/emc/vmdirect/bin/vproxymgmt get -list**

Transparent Snapshot Data Mover protection mechanism

The **Protection Engines** window in the PowerProtect Data Manager UI includes a pane for **Transparent Snapshot Data Movers**. Transparent Snapshot Data Mover (TSDM) is a protection mechanism that is introduced in PowerProtect Data Manager 19.9 for data movement during virtual machine protection operations. Previously, the only protection mechanism available in PowerProtect Data Manager for virtual machine protection was the VMware vStorage API for Data Protection (VADP).

A vSphere Installation Bundle (VIB) is included with the software installation and update packages for PowerProtect Data Manager 19.9 to facilitate the use of TSDM, and is enabled at the vCenter level upon the PowerProtect Data Manager 19.9 installation or update. The VIB installation occurs automatically at the cluster level when a virtual machine protection policy is created, with no requirement to restart the ESXi hosts or put the hosts into maintenance mode. Any new virtual machine protection policies use TSDM as the default protection mechanism instead of VADP, provided that the vCenter/ESXi Server that hosts the virtual machines is a minimum version of 7.0 U3.

The **Transparent Snapshot Data Movers** pane provides a hierarchy view of the vCenter Server asset sources that have been added in PowerProtect Data Manager. Use this view to determine if the vCenter/ESXi is enabled for VIB management, and if the hosts have the VIB installed or are eligible for VIB installation. A vSphere host cluster can have one of the following statuses:

- **Installed**—The VIB installation on this vSphere host is completed, and TSDM is enabled as the default protection mechanism for the virtual machines on the vSphere host.
- **Ready for install**—The vSphere host requirements for VIB installation have been met, and the installation will proceed automatically on the vSphere host when a virtual machine running on the cluster is added to a protection policy.
- **Ready for upgrade**—This status displays when the VIB is installed on the vSphere host and PowerProtect Data Manager is upgraded, but the VIB is being managed manually. In this case, the VIB will not be upgraded automatically on the vSphere host.
- **Not eligible**—The vSphere host does not meet the requirements for VIB installation. When TSDM cannot be used, the VADP protection mechanism is used for virtual machine protection operations on this host.
- **Failed**—The VIB installation on the vSphere host did not complete successfully. The **Jobs** window provides more information about the issue that caused the failure.

Use the filter icon in the status column to display only vSphere hosts with a certain status. For example, you can choose to display only hosts that are ready for VIB installation or upgrade.

When the VIB installation is started, the **Protection Engines** window updates to display the progress. Also, an entry for the job **Performing Host Configuration (vib_install)** appears in the **Jobs** window.

NOTE: Any virtual machine assets that were added to a virtual machine protection policy in PowerProtect Data Manager 19.8 and earlier currently use the VADP protection mechanism. After the VIB installation on the vSphere host that contains these virtual assets, you can migrate these assets to the TSDM protection mechanism. [Migrating assets to use the Transparent Snapshot Data Mover](#) on page 71 provides more information.

Disable or re-enable VIB on an ESXi host

In the PowerProtect Data Manager UI, you can disable VIB management on a vCenter to prevent automatic installation or update of the VIB on the ESXi host. To disable VIB management on the vCenter:

1. Go to **Infrastructure > Protection Engines**, and then select the **Transparent Snapshot Data Movers** pane.
2. Hover over the **Enabled** icon to the right of the vCenter, and then click **Disable**.

To re-enable VIB management on a vCenter that currently has the VIB disabled:

1. Hover over the icon to the right of the host, and then click **Enable**.

If a VIB installation or update is required, the status indicates **Ready for install** or **Ready for upgrade**.

2. Select the checkbox next to this host and click **Install** to manually perform the VIB install or update, or wait for the automatic VIB installation.
3. When performing a manual VIB installation, if one or more of the selections are not eligible or the VIB is already installed, a dialog appears. Click **OK** to proceed.

Migrating assets to use the Transparent Snapshot Data Mover

Transparent Snapshot Data Mover (TSDM) is the recommended protection mechanism for environments with vCenter/ESXi version 7.0 U3 and later installed, and is the default protection mechanism used for virtual machine assets protected by virtual machine crash-consistent policies in PowerProtect Data Manager 19.9 and later, provided that the policy is configured with the following options:

- **Performance** optimization mode.
- **Exclude swap files from backup** is off.
- **Enable guest file system quiescing** is off.

For existing virtual machine crash-consistent policies created with PowerProtect Data Manager version 19.8 and earlier, modifying the policy options to meet these requirements will migrate virtual machines on vSphere version 7.0 U3 and later clusters managed by a vCenter Server running version 7.0 U3 and later to use the TSDM protection mechanism.

You can also migrate virtual machine assets from the VADP protection mechanism to the TSDM protection mechanism by using the **Infrastructure > Assets** window of the PowerProtect Data Manager UI.

Before migrating assets to use TSDM, the vSphere Installation Bundle (VIB) is required. This installation occurs automatically, unless the use of TSDM is disabled on the vCenter Server asset source. Go to **Infrastructure > Protection Engines**, select the **Transparent Snapshot Data Movers** pane, and verify that the VIB is enabled on the vCenter. You can also expand the vCenter hierarchy view to confirm that the VIB installation has occurred on the vSphere hosts. [Transparent Snapshot Data Mover protection mechanism](#) on page 70 provides more information.

Migrate asset protection mechanism from VADP to TSDM

To migrate VADP virtual machine assets to use TSDM in the PowerProtect Data Manager UI:

1. Go to **Infrastructure > Assets** and select the **Virtual Machine** tab.
2. Filter the view to display the **Protection Mechanism** column.
3. Select one or more virtual machine assets with the VADP protection mechanism.
4. Select **More Actions > Protection Mechanism > Migrate to TSDM**.

Migrating assets to use the TSDM protection mechanism forces a new, full backup of these assets. This backup may take several minutes.

Adding a Cloud Snapshot Manager tenant


After you enable the Cloud Snapshot Manager tenant asset-source with PowerProtect Data Manager, you use the **Asset Sources** window in PowerProtect Data Manager to add a Cloud Snapshot Manager tenant to the PowerProtect Data Manager environment.

Adding a Cloud Snapshot Manager tenant is required if you want to view Cloud Snapshot Manager jobs, alerts, and reports from a consolidated PowerProtect Data Manager dashboard.

Add a Cloud Snapshot Manager Tenant

Perform the following steps to add a Cloud Snapshot Manager tenant as an asset source in the PowerProtect Data Manager UI.

Prerequisites

- Ensure that the asset source is enabled. [Enable an asset source](#) on page 60 provides instructions.
- Log in as a user with the Administrator role. Only the Administrator role can manage asset sources.
- The PowerProtect Data Manager server has Internet access and is able to reach <https://ssgosge.emc.com>.
 **NOTE:** If this access is removed during normal operation, any existing Cloud Snapshot Manager information will continue to be displayed in the **Dashboard** window, but there will be no updates until Internet access is restored.
- This procedure requires the entry of values specific to Cloud Snapshot Manager. For more information, see the *PowerProtect Cloud Snapshot Manager Online Help*.

Steps

1. From the left navigation pane, select **Infrastructure > Asset Sources**.
The **Asset Sources** window appears.
2. Select the **Cloud Snapshot Manager** tab.
3. Click **Add**.
The **Add Cloud Snapshot Manager Account Details** dialog displays.
4. In the **Name** field, enter a descriptive name for the Cloud Snapshot Manager tenant.
5. In the **Tenant ID** field, enter the Cloud Snapshot Manager tenant ID.
6. Click the drop-down control next to **Cloud Snapshot Manager Credentials**, and then click **Add Credentials**.
 - a. In the **Name** field, enter the name of the Cloud Snapshot Manager tenant credentials.
 - b. In the **Client ID** field, enter the ID of the Cloud Snapshot Manager tenant.
 - c. In the **Client Secret** field, enter the secret of the Cloud Snapshot Manager tenant.
 - d. Click **Save**.
7. Click **Save**.

Managing Protection Policies

Topics:

- [Protection policies](#)
- [Before you create a protection policy](#)
- [Supported enhanced VMware topologies for virtual-machine protection](#)
- [Add a protection policy for virtual-machine protection](#)
- [Add a Cloud Tier schedule to a protection policy](#)
- [Manual backups of protected assets](#)
- [Manual replication of protected assets](#)
- [Manual Cloud Tiering of protected assets](#)
- [Editing a protection policy](#)
- [View assets assigned to a protection policy](#)
- [Extended retention](#)
- [Edit the retention period for backup copies](#)
- [Delete backup copies](#)
- [Removing expired backup copies](#)
- [Removing assets from PowerProtect Data Manager](#)
- [Export protection](#)
- [Disable a protection policy](#)
- [Delete a protection policy](#)
- [Add a Service Level Agreement](#)
- [Export Asset Compliance](#)
- [Protection rules](#)

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 policy type has its own set of user objectives.

Only the Administrator role can create or edit protection policies.

You can create protection policies for the following asset types:

- VMware virtual machines
- Microsoft Exchange and SQL databases
- Oracle databases
- SAP HANA databases
- File systems
- Kubernetes clusters
- Storage groups
- Network-attached storage (NAS)

This guide provides steps only for virtual-machine protection policies. For other policy types, refer to the individual user guides.

Before you create a protection policy

Consider the following best practices before creating a protection policy.

- An asset can be protected by only one policy at a time. Assets can be moved from one policy to another policy based on the priority of protection rules. In cases where protection rules result in assets moving from one policy to another, any assets that were manually selected for inclusion in the policy, however, will not be moved to a different policy.

i NOTE: If a SQL Server is hosted on a virtual machine, you can protect the SQL database with an application-consistent backup without interfering with the SQL agent-based backup.

- When creating a policy, limit the number of database assets within the policy to under 500 and stagger the start time of replication policies to avoid potential replication failures.
- Before adding replication to a protection policy, ensure that you add remote protection storage as the replication location. [Add protection storage](#) on page 39 provides detailed instructions about adding remote protection storage.
- Before you perform any backups on a weekly or monthly schedule from the protection policy, ensure that the PowerProtect Data Manager time zone is set to the local time zone.

Understanding backup terminology and managing backup frequency

When scheduling backups in a protection policy, be aware of the following:

- Different backup policy types can use different terminology to describe available backup levels. This terminology can differ not only between policy types, but also from traditional terminology.
- To avoid high CPU usage that can lead to failure issues, do not schedule backups more often than recommended.

Refer to the following table to understand the different backup levels provided by each protection policy and to manage backup frequencies.

Table 26. Backup terminology and frequency

Protection-policy backup types	Available backup levels	Description	Equivalent traditional terminology	Minimum frequency recommendation
VMware application-aware	Full	Backs up all the blocks.	Full	Monthly
	Synthetic Full	Backs up only the blocks that have changed since the last synthetic-full or full backup, and then performs an operation to merge those changes with the last synthetic-full or full backup in order to produce a full backup in storage. Only the changed blocks are actually copied over the network, but the result is still a full backup in storage.	A differential backup is performed, followed by a merge operation that produces a full backup in storage.	12 hours
	Log	Backs up the transaction logs.	-	30 minutes
VMware crash-consistent	Full	Backs up all the blocks.	Full	Monthly
	Synthetic Full	Backs up only the blocks that have changed since the last synthetic-full or full backup, and then performs an operation to merge those changes with the last synthetic-full or full backup in order to produce a full backup in storage. Only the changed blocks are actually copied over the network, but the result is still a full backup in storage.	A differential backup is performed, followed by a merge operation that produces a full backup in storage.	12 hours

Table 26. Backup terminology and frequency (continued)

Protection-policy backup types	Available backup levels	Description	Equivalent traditional terminology	Minimum frequency recommendation
Kubernetes crash-consistent	Full	Backs up the namespace metadata and persistent volumes.	Full	Daily
	Synthetic Full	Backs up the namespace metadata, the blocks that have changed for persistent volumes on VMware first-class disks since the last synthetic-full or full backup, and all other persistent volumes in full. Although not all data has actually been copied over the network, the result is still a full backup in storage.	A combination of full and differential backups are performed, followed by a merge operation that produces a full backup in storage.	12 Hours
File System centralized	Full	Backs up all the data.	Full	Monthly
	Synthetic Full	Backs up only the data that has changed since the last synthetic-full or full backup, and then performs an operation to merge those changes with the last synthetic-full or full backup in order to produce a full backup in storage. Only the changed blocks are actually copied over the network, but the result is still a full backup in storage.	A differential backup is performed, followed by a merge operation that produces a full backup in storage.	12 hours
Exchange centralized	Full	Backs up all the data.	Full	Weekly
	Synthetic Full	Backs up only the data that has changed since the last synthetic-full or full backup, and then performs an operation to merge those changes with the last synthetic-full or full backup in order to produce a full backup in storage. Only the changed blocks are actually copied over the network, but the result is still a full backup in storage.	A differential backup is performed, followed by a merge operation that produces a full backup in storage.	12 hours
SQL centralized	Full	Backs up all the data.	Full	Daily
	Differential	Backs up only the data that has changed since the last differential backup, or the last full backup if there are no other differential backups.	A differential backup is performed, followed by a merge operation that produces a full backup in storage.	12 hours
	Log	Backs up the transaction logs.	-	30 minutes
Oracle centralized	Full	Backs up all the data.	Full	Daily
	Incremental Cumulative	Backs up only the data that has changed since the last full backup.	Differential	12 hours

Table 26. Backup terminology and frequency (continued)

Protection-policy backup types	Available backup levels	Description	Equivalent traditional terminology	Minimum frequency recommendation
	Incremental Differential	Backs up only the data that has changed since the last incremental differential backup, or the last full backup if there are no other incremental differential backups.	Incremental	6 hours
	Log	Backs up the archived logs.	-	30 minutes
SAP HANA centralized	Full	Backs up all the data.	Full	Daily
	Differential	Backs up only the data that has changed since the last full backup.	Differential	12 hours
	Incremental	Backs up only the data that has changed since the last incremental backup, or the last full backup if there are no other incremental backups.	Incremental	6 hours
VMAX storage group centralized	Full	Backs up all the blocks.	Full	Daily
	Synthetic Full	Backs up only the blocks that have changed since the last synthetic-full or full backup, and then performs an operation to merge those changes with the last synthetic-full or full backup in order to produce a full backup in storage. Only the changed blocks are actually copied over the network, but the result is still a full backup in storage.	A differential backup is performed, followed by a merge operation that produces a full backup in storage.	12 hours

NOTE: In some situations, a full backup might be performed even though a synthetic-full backup was scheduled. Possible reasons for this include, but are not limited to, the following:

- There is no existing full backup.
- The size of a volume has changed.
- There has been a file path change.
- The asset host has been rebooted.

Supported enhanced VMware topologies for virtual-machine protection

PowerProtect Data Manager provides protection for clustered ESXi server storage, networking, and enterprise management. Understanding what topologies are supported in these environments aids in the design of your network infrastructure.

Supported enhanced topologies

Supported topologies of clustered ESXi server storage, networking, and enterprise management include the following:

- vSAN operations
- NSX-T port groups

- Enhanced Link Mode vCenter servers

For more information see the [E-Lab Navigator](#).

vSAN operations

Standard clusters, stretched clusters, two-node clusters, and HCI Mesh datastores support the following operations:

- Backing up and restoring virtual machines
- Search Engines
- VM Direct Engines
- HA failover of Search Engines and VM Direct Engines
- Post-failover protection

NSX-T port groups

PowerProtect Data Manager supports the use of NSX-T with up to 2,000 port groups. These can be default VDS port groups or N-VDS port groups, and they support the following components:

- PowerProtect Data Manager servers
- VM Direct Engines
- Search nodes
- Workload virtual machines

Enhanced Link Mode vCenter servers

Enhanced Linked Mode connects multiple vCenter Server systems together by using one or more Platform Services Controllers (PSCs). PowerProtect Data Manager supports the protection of workload virtual machines running inside Enhanced Linked Mode vCenter servers. This protection also applies during and after any vMotion operation of the virtual machines.

To support virtual machine protection workflows for vCenter Servers that are in Enhanced Linked Mode, PowerProtect Data Manager requires you to add all of the linked vCenters as asset sources, and also to install the PowerProtect **vSphere Plugin** on all of these vCenters

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 and replicate. Perform the following steps to create a virtual-machine protection policy in the PowerProtect Data Manager UI.

Prerequisites

It is recommended that you distribute virtual-machine asset protection workloads over multiple ESXi hosts so that you do not exceed the ESXi Network Block Device (NBD) session limit. If the limit is reached, you can manage the workload by deploying an external VM Direct Engine on the host or cluster using **Hot Add** transport mode. Also, Dell Technologies recommends during policy configuration to assign virtual machines to a protection policy based on logical grouping to allow for better scheduling of backups. Grouping helps avoid resource contention and creates more organized logs for review.

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 e-Lab Navigator, available at <https://elabnavigator.emc.com/eln/modernHomeDataProtection>.
- The virtual machine has direct access to the DD 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 is limited to the local system Administrator or the domain Administrator. This user requires both Microsoft Windows administrative rights and Microsoft SQL Server login and sysadmin rights.

- 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.
- To protect virtual machines that use virtualization-based security (VBS) and virtual Trusted Platform Module 2.0 (vTPM), vCenter 7.0 U1 or later is required.

If applicable, complete all of the virtual network configuration tasks before you assign any virtual networks to the protection policy.

Chapter [Managing Storage](#) on page 38 provides more information about working with storage units, including applicable limitations and security considerations.

Before performing any backups on a weekly or monthly schedule from the protection policy, ensure that the PowerProtect Data Manager time zone is set to the local time zone.

About this task

For virtual-machine protection policies, data is moved using one of two types of protection mechanisms:

- **Transparent Snapshot Data Mover**—Starting in PowerProtect Data Manager version 19.9, Transparent Snapshot Data Mover (TSDM) is the default protection mechanism that is used for crash-consistent virtual-machine policies when the following requirements are met:
 - vCenter/ESXi version 7.0 U3 and later is installed in the environment.
 - The protection policy uses **Performance** optimization mode, with the **Exclude swap files from backup** and **Enable guest file system quiescing** checkboxes cleared.
- **VADP**—VMware vStorage API for Data Protection (VADP) is the protection mechanism that is used for application aware virtual-machine policies and crash-consistent policies that do not meet the TSDM software requirements. VADP is the only protection mechanism available in PowerProtect Data Manager versions 19.8 and earlier.

The section [Transparent Snapshot Data Mover protection mechanism](#) on page 70 provides more information about TSDM.

Steps

1. From the left navigation pane, 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 must provide Windows account credentials for the virtual machine. You can provide the credentials at the protection-policy level 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.

By default, quiescing is automatically performed for the guest file system on the virtual machine. Quiescing ensures that the data within the guest file system is in a state that is appropriate for backups. If the file system cannot be quiesced on the first attempt, then the snapshot and backup are performed without quiescing.

VMware Tools is used to quiesce the file system in the guest operating system. The [VMware documentation](#) provides more information.

5. On the **Assets** page, select the assets for inclusion in this policy by choosing one of the following options from the list:
 - **View by Host**—This option enables you to view all assets within a specific host, and then select individual assets or a group of assets at a host or container level for policy inclusion. For example:
 - Select a stand-alone host to include all assets under this host.

NOTE: If you select a host in a cluster, no assets are selected. For a host in a cluster, ensure that you select the cluster or other containers (for example, a resource pool or vApp) under the cluster host.

- Expand the tree and select a container level in the vCenter hierarchy (for example, the data center, cluster, host, or resource pool) to include all assets under that level. If assets at any level are protected by another policy, a label with the name of that policy appears next to the level.

NOTE: VMs created by the vSphere Cluster Service (vCLS) are managed by VMware, and do not require PowerProtect Data Manager protection. Even when selected as part of a container, they are automatically excluded from protection. The `vmdm-discovery.log` provides a list of vCLS VMs that are excluded from protection.

When you select a container level in the **View by Host** view, a protection rule is automatically created to ensure that these container level selections will be retained, even if changes occur from movements within the vSphere environment or the names of resource pools or folders change. This rule is managed by the PowerProtect Data Manager system, and cannot be modified. The rule will also be updated automatically if you make changes to container selections when editing the policy, or when assets are moved into or out of a selected container.

To view this rule after policy creation, go to **Protection > Protection Rules**. The name in the **Protection Rule Name** column for this new rule matches the policy name.

If this new rule results in an overlap of protection with an existing rule, you can resolve these conflicts by changing the policy protection rule priority in the **Selection Overlap** page. Step 7 on page 79 provides more information.

NOTE: The behavior of automatic rule creation that allows assets to move into or out of policies can only be modified in the REST API. After updating from a previous release, if **View by Host** is not visible you can enable this view by manually changing the `/api/v2/common-settings/DYNAMIC_FILTER_SETTING`. The [PowerProtect Data Manager Public REST API documentation](#) provides instructions.

- Expand the tree and select individual assets within containers.

When you select individual assets within this view, these selections are considered static, and no protection rule is automatically created. In cases where protection rules result in assets moving from one policy to another, any assets that are manually selected for inclusion in the policy will not be moved to a different policy.

- View Asset Table**—This option enables you to view all unprotected assets in the vCenter within a table, and then select individual unprotected assets that you want to back up as part of this protection policy. In cases where protection rules result in assets moving from one policy to another, any assets that are manually selected for inclusion in the policy will not be moved to a different policy.

When you select a virtual-machine asset in this view, a dialog displays indicating that you can exclude virtual disks (VMDKs) from protection of these assets. To dismiss the dialog for other selections, select the check box and click **OK**.

Both views provide additional information about the virtual machines, such as any currently associated tags, protection rules, and whether the virtual machine is already assigned to another policy, to help you identify which assets you want to add. If the virtual machines that you want to protect are not listed, use the **Search** box to search by asset name.

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.

- Optionally, if you want to exclude nonproduction VMDKs such as network shares or test disks from a protection policy:
 - Select the virtual-machine asset from the list, and then click **Manage Exclusions** in the **Disk Excluded** column. The **Exclude Disks** dialog box appears. By default, the slider next to each VMDK is set to **Included**.
 - For each disk that you want to exclude, move the slider to the right. The status updates to **Excluded**.

NOTE: For PowerProtect Data Manager version 19.3, a virtual machine with disk exclusion and Cloud Disaster Recovery (DR) cannot co-exist in the same protection policy. If you exclude disks from a virtual-machine protection policy, Cloud DR is not supported.
 - Click **Save**. The **Assets** page updates to indicate the number of disks for that particular asset that will be excluded from the protection policy.
- Click **Next**.

If any virtual objects or assets that were selected in the previous page overlap with assets that are already protected by another policy, the **Selection Overlap** page appears. Overlap can occur, for example, when two policies (the new policy and an existing policy) use the **View by Host** view for asset selection by container level.

- a. To switch protection of any virtual objects listed in the **Protection Priority Overlap** table from an existing policy, update the **Policy Priority** field to a level equal to or higher than the other policy currently protecting these objects. The lower the value, the higher the priority. For example, **1** is the highest priority. When you change this value, the priority of the rule that is associated with this policy is also changed.
- b. To switch protection of any assets that are listed in the **Asset Protection Overlap** table to this policy, select the checkbox next to one or more assets. Note that selecting these assets for inclusion in this policy removes the assets from the other policy.

When you change the priority or the selected assets, the protection rule is updated automatically.

8. Click **Next**.
The **Objectives** page appears.
9. On the **Objectives** page, select a policy-level Service Level Agreement (SLA) from the **Set Policy Level SLA** list, or select **Add** to open the **Add Service Level Agreement** wizard and create a policy-level SLA.
[Add a Service Level Agreement](#) on page 102 provides instructions.
10. Click **Add** under **Primary Backup**.
The **Add Primary Backup** dialog appears.
11. On the **Schedules** pane of the **Add Primary Backup** dialog:
 - a. Specify the following fields to schedule the synthetic full backup of this protection policy:
 - **Create a Synthetic Full...**—Specify how often to create a synthetic full backup. A **Synthetic Full** backs up only the changed blocks since the last backup to create a new full backup.
 - **Retain For**—Specify the retention period for the synthetic full backup.

You can extend the retention period for the latest primary backup copy by using the **Extend Retention** schedule. For example, your regular schedule for daily backups can use a retention period of 30 days, but you can apply extended retention to keep the full backups taken on Mondays for 10 weeks. Step 14 on page 81 provides instructions.

i **NOTE:** For database backups, PowerProtect Data Manager chains the dependent backups together. For example, the synthetic full or transaction log backups are chained to their base full backup. The backups do not expire until the last backup in the chain expires. This ensures that all synthetic full and transaction log backups are recoverable until they have all expired.

- **Start** and **End**—For the activity window, specify a time of day to start the synthetic full backup, and a time of day after which backups cannot be started.

i **NOTE:** Any backups started before the **End Time** occurs continue until completion.


- Click **Save** to save and collapse the backup schedule.
- b. Click **Add Backup** if you want to periodically force a full (level 0) backup, and then specify the following fields to schedule the full backup of this protection policy:

i **NOTE:** When you select this option, the backup chain is reset.

 - **Create a Full...**—Specify whether you want to create a weekly or monthly full backup.
 - **Repeat on**—Depending on the frequency of the full backup schedule, specify the day of the week or the date of the month for the full backup.
 - **Retain For**—Specify the retention period for the full backup. This can be the same value as the synthetic full backup schedule, or a different value.
 - **Start** and **End**—For the activity window, specify a time of day to start the full backup, and a time of day after which backups cannot be started.

i **NOTE:** Any backups started before the **End Time** occurs continue until completion.

 - Click **Save** to save and collapse the backup schedule.
 - c. For virtual-machine application-aware protection policies, click **Add Backup** to create a log backup, and then specify the following fields:
 - **Create a Log...**—For application-aware protection policies, specify the interval in minutes for log generation.
 - i** **NOTE:** For 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.
 - **Retain For**—Specify the retention period for the log backup. This can be the same retention value specified for the synthetic full or full schedule, or a different value.

 **NOTE:** Setting a shorter retention period for log backups than the full backup can result in data loss and the inability to restore point-in-time copies.


- **Start** and **End**—For the activity window, specify a time of day to start the log backup, and a time of day after which log backups cannot be started.

 **NOTE:** Any backups started before the **End Time** occurs continue until completion.

- Click **Save** to save and collapse the backup schedule.

12. On the **Target** pane of the **Add Primary Backup** dialog, specify the following fields:


- a. **Storage Name**—Select a backup destination from the list of existing protection storage systems, or select **Add** to add a system and complete the details in the **Storage Target** window.

 **NOTE:** The **Space** field indicates the total amount of space, and the percentage of available space, on the protection storage system.

- b. **Storage Unit**—Select whether this protection policy should use a **New** storage unit on the selected protection storage system, or select an existing storage unit from the list. Hover over a storage unit to view the full name and statistics for available capacity and total capacity, for example, **testvmplc-ppdm-daily-123ab (300 GB/1 TB)**

When you select **New**, a new storage unit in the format *policy name host name unique identifier* is created in the storage system upon policy completion. For example, **testvmplc-ppdm-daily-123cd**.

- c. **Network Interface**—Select a network interface from the list, if applicable.
- d. **Retention Lock**—Move the **Retention Lock** slider to the right to enable retention locking for these backups on the selected system. PowerProtect Data Manager uses Governance mode for retention locking, which means that the lock can be reverted at any time if necessary. Moving the **Retention Lock** slider on or off applies to the current backup copy only, and does not impact the retention lock setting for existing backup copies.


 **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 enable **Retention Lock** for a replicated backup, ensure that you set the **Retain For** field in the **Add Replication** backup schedule dialog to a minimum number of 14 days so that the replicated backup does not expire before the primary backup.

- e. **SLA**—Select an existing service level agreement that you want to apply to this schedule from the list, or select **Add** to create an SLA within the **Add Service Level Agreement** wizard.

[Add a Service Level Agreement](#) on page 102 provides instructions.

13. Click **Save** to save your changes and return to the **Objectives** page.

The **Objectives** page updates to display the name and location of the target storage system under **Primary Backup**.

 **NOTE:** After completing a backup schedule, you can change any schedule details by clicking **Edit** next to the schedule.


14. Optionally, extend the retention period for the latest primary backup copy:

[Extended retention](#) on page 93 provides more information about **Extend Retention** functionality.

- a. Click **Extend Retention** next to **Primary Backup**. An entry for **Extend Retention** is created below **Primary Backup**.
- b. Under **Extend Retention**, click **Add**. The **Add Extended Retention** dialog appears.
- c. **Retain the next scheduled full copy every...**—Specify a weekly, monthly, or yearly recurrence for the extended retention backup schedule.
- d. **Repeat on**—Depending on the frequency of the full backup schedule, specify the day of the week, the date of the month, or the date of the year that the extended retention backup will occur.
- e. **Retain For**—Specify the retention period for the backup. You can retain an extended retention backup for a maximum of 70 years.
- f. Click **Save** to save your changes and return to the **Objectives** page.

15. Optionally, replicate the full and synthetic full backups to a remote storage system:

- a. Click **Replicate** next to **Primary Backup** or **Extend Retention**. An entry for **Replicate** is created to the right of the primary or extended retention backup schedule.

 **NOTE:** PowerProtect Data Manager supports replicating an extended retention backup only if the primary backup already has one or more replication stages. Also, for replication of an extended retention backup, you can only select the protection storage systems that are used by the replication stages based on the primary stage.

For example, if there are 6 systems available (DD001-DD006), and the primary backup is on DD0001:

- Replicate1 based on the primary backup is replicated to DD002
- Replicate2 based on the primary backup is replicated to DD003

- Extended retention backup is backed up to DD001
- Replicate3 based on the extended retention backup must be replicated to DD002 or DD003.

b. Under **Replicate**, click **Add**. The **Add Replication** dialog appears.

NOTE: To enable replication, ensure that you add remote protection storage as the replication location. [Add protection storage](#) on page 39 provides detailed instructions about adding remote protection storage.

c. Complete the schedule details in the **Add Replication** dialog, and then click **Save** to save your changes and return to the **Objectives** page.

The schedule frequency can be every day, week, month, or x hours for replication of the primary backup, and every day, week, month, year, or x hours for replication of the extended retention backup. For daily, weekly, and monthly schedules, the numeric value cannot be modified. For hourly, however, you can edit the numeric value. For example, if you set **Create a Full backup every 4 hours**, you can set a value of anywhere 1 to 12 hours.

All replication copies of the primary backup schedule will use the same retention period, and by default, this retention period is inherited from the **Retain For** value of the synthetic full backup schedule. To specify a different retention period for all of the replication copies of this primary backup schedule, click **Edit**, change the value in the **Retain For** field, and then click **Save**. This retention period will be applied to all of the replicated copies (synthetic full and full) of this primary backup schedule.

When creating multiple replication copies of the same protection policy, Dell Technologies recommends selecting a different storage system for each copy.

16. Optionally, to move backups from DD storage to Cloud Tier, add a Cloud stage for the primary, replication, or extended retention schedule:

a. Click **Cloud Tier** next to **Primary Backup** or **Extend Retention** or, if adding a Cloud stage for a replication schedule that you have added, click **Cloud Tier** under **Replicate**. An entry for **Cloud Tier** is created to the right of the primary or extended retention backup schedule, or below the replication schedule.

b. Under the entry for **Cloud Tier**, click **Add**.

The **Add Cloud Tier Backup** dialog appears, with summary schedule information for the parent node to indicate whether you are adding this Cloud Tier stage for the primary backup schedule, the extended retention backup schedule, or the replication schedule.

c. Complete the schedule details in the **Add Cloud Tier Backup** dialog, and then click **Save** to save your changes and return to the **Objectives** page.

[Add a Cloud Tier schedule to a protection policy](#) on page 86 provides detailed instructions for adding a Cloud stage for a primary, replication, or extended retention schedule.

NOTE: In order to move a backup or replica to Cloud Tier, schedules must have a retention time of 14 days or more. Also, discovery of protection storage that is configured with a Cloud unit is required.

17. Optionally, if **Cloud Disaster Recovery** is configured in the **Infrastructure > Storage** window, you can add a Cloud DR stage for virtual-machine protection policies:

a. Click **Cloud DR** next to **Primary Backup** or **Extend Retention** or, if adding a Cloud stage for a replication schedule that you have added, click **Cloud DR** under **Replicate**. An entry for **Cloud DR** is created to the right of the primary or extended retention backup schedule, or below the replication schedule.

b. Under the entry for **Cloud DR**, click **Add**.

The **Add Cloud DR Backup** dialog appears, with summary schedule information for the parent node to indicate whether you are adding this Cloud DR stage for the primary backup schedule, the extended retention backup schedule, or the replication schedule.

c. Complete the schedule details in the **Add Cloud DR Backup** dialog, and then click **Save** to save your changes and return to the **Objectives** page.

The *PowerProtect Data Manager Cloud Disaster Recovery Administration and User Guide* provides detailed instructions for adding a Cloud DR stage for a primary, replication, or extended retention schedule.

18. Click **Next**.

The **Options** page appears.

19. On the **Options** page:

a. For **Optimize For**, select from one of the following backup optimization modes:

- **Performance**—Optimize for backup and replication speed. Selecting this mode results in more storage consumption. Previous versions of PowerProtect Data Manager used this option by default.

When using the **Transparent Snapshot Data Mover** protection mechanism, select **Performance** optimization mode.

- **Capacity**—Optimize for backup size. Selecting this mode results in less storage consumption, but backups take longer to complete.

NOTE: Changing the optimization mode after the first backup of the protection policy forces the next backup to be a full backup, and results in increased storage capacity usage due to differences in how each mode uses data deduplication. This increase continues until all backups performed using the previous optimization mode expire and have been deleted.

- b. **Exclude swap files from backup**—Select to exclude the C:\swapfile.sys, C:\pagefile.sys, and C:\hiberfil.sys swap and memory files of Microsoft Windows virtual machines, in the virtual-machine backup. By default, this checkbox is cleared.

When using the **Transparent Snapshot Data Mover** protection mechanism, do not select the **Exclude swap files from backup** checkbox.

NOTE: Including swap and memory files in a backup unnecessarily increases the size of the backup and the time to RTO during recovery. These files are rebuilt by the Microsoft Windows operating system upon restart, and not required for recovery.

- c. **Enable indexing for file search and restore**—Select to enable indexing. This option is visible only upon activating the search cluster node.
- d. **Enable guest file system quiescing**—Select to enable **VMware Tools** to quiesce the file system during crash-consistent virtual-machine backups.

When using the **Transparent Snapshot Data Mover** protection mechanism, do not select the **Enable guest file system quiescing** checkbox.

20. Click **Next**.

The **Summary** page appears.

21. Review the protection policy group configuration details. Except for the protection policy type, you can click **Edit** next to any details to change the protection policy information. When satisfied with the details, click **Finish**. An informational message appears to confirm that PowerProtect Data Manager has saved the protection policy.

When the new protection policy is created and assets are added to the protection policy, PowerProtect Data Manager performs backups according to the backup schedule.

For virtual machines, if you have not yet added a VM Direct Engine, the backup is performed using the embedded VM Direct Engine that is included with PowerProtect Data Manager. Subsequent backups are performed according to the schedule specified.

NOTE: If the target virtual-machine datastore for backup is running low on free space and the datastore free space threshold is configured in **vCenter Settings**, a warning message appears or a backup failure occurs. When the **Datastore Free Space Warning Threshold** is reached, the backup proceeds with a warning message in the logs. When the **Datastore Free Space Failure Threshold** is reached, the backup fails.

To check the warning and failure threshold values, select **Infrastructure > Asset Sources** and click the **vCenter** tab. Click the gear icon to open the **vCenter Settings** dialog.

22. 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.


Managing virtual-machine backups

The following sections describe the options that are available for virtual-machine assets that are backed up as part of a protection policy.

Add and remove the credentials for virtual-machine assets

You can optionally add and remove the credentials for multiple virtual-machine assets at the same time in the PowerProtect Data Manager UI. With previous versions, you could add and remove the credentials for one virtual-machine asset at a time.

About this task

 **NOTE:** The asset-level credentials take precedence over policy-level credentials for virtual machines. Asset-level credentials have the highest precedence. Virtual machines do not support the asset source-level (host) credentials.

Use the following procedure to add or remove one or more credentials for virtual-machine assets.

Steps

1. From the PowerProtect Data Manager UI, select **Infrastructure > Assets**, and then click the **Virtual Machine** tab.
2. Select one or more assets by clicking the checkbox next to each required asset name.
3. Select **More Actions > Set Credential**.
4. In the **Set Credential** dialog box, add or remove the credentials for the selected virtual-machine assets:
 - To add the credentials for the assets, select the appropriate value from the drop-down list in the **Credential** field:
 - To create new credentials, select **Create New**.
In the **Add Credentials** dialog box that appears, specify the required field values and then click **Save**.
 - To add existing credentials, select the credentials name from the credentials list.
 - To remove the credentials for the assets, select **Remove Credentials**.
5. Click **Save** in the **Set Credential** dialog box.

Results

After you add the credentials by using this procedure, the asset-level credentials are used for the selected assets during the virtual-machine centralized backups, overriding the policy-level credentials.

Enable or disable Changed Block Tracking (CBT)

The Changed Block Tracking (CBT) feature is used to identify areas of the virtual-machine backup that have changed since the last backup and only process those changed areas during the next backup. CBT is enabled by default.

About this task

To set Changed Block Tracking (CBT) for virtual machines, complete the following steps:

Steps

1. From the PowerProtect Data Manager UI, select **Infrastructure > Assets**.
2. From the **Assets** window, select the **Virtual Machine** tab. If a policy has been assigned, the table lists the virtual-machine assets that have been discovered in the vCenter, along with the associated protection policy.
3. Select one or more virtual-machine assets from the list, and click **More Actions > Changed Block Tracking**.
The **Changed Block Tracking** dialog box appears.
4. Clear the check box to disable CBT, or select the check box to enable CBT.
In some cases, CBT can cause backups to take longer than expected if there are high change rates on the virtual machine. You can disable CBT for virtual machines if the backups are taking too long to complete. Also, if you encounter an issue with CBT, you can disable it on the virtual machine.

NOTE: If CBT is enabled in PowerProtect Data Manager but is disabled in VMware vSphere, PowerProtect Data Manager tries to back up the virtual machine with CBT enabled. If PowerProtect Data Manager cannot enable CBT, the backup completes with a warning that indicates CBT data is not available.

5. Click **Save**.

NOTE: When CBT is disabled for a virtual machine, subsequent backups no longer use CBT.

More options for managing virtual-machine backups

After you create a virtual-machine protection policy, additional options become available for virtual-machine assets that are backed up as part of the policy.

To access these options:

1. From the PowerProtect Data Manager UI, select **Infrastructure > Assets**.
2. From the **Assets** window, select the **Virtual Machine** tab. If a policy has been assigned, the table lists the virtual-machine assets that have been discovered in the vCenter, along with the associated protection policy.

NOTE: You can click the link in the **Disk Excluded** column next to a virtual-machine asset to view VMDKs that have been excluded from the protection policy. You cannot, however, edit disk inclusion or exclusion from this window. To change the disks that are excluded for a protected asset, select the policy from the **Protection Policies** window and click **Edit**.

3. Select a protected asset from the table, and then click **View Copies**. The **Copy Locations** pane identifies where the backups are stored.
4. 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 of backup copies to extend or shorten the amount of time that backups are retained—Select one or more backup copies from the table and click **Edit Retention**.
 - To select a calendar date as the expiration date for backups, select **Retention Date**.
 - To define a fixed retention period in days, weeks, or months after the backup is performed, select **Retention Value**. For example, you could specify that backups expire after 6 months.
- NOTE:** When you edit the retention period for copies that are retention locked, you can only extend the retention period.
- Delete a backup copy—If you no longer require a copy and the retention lock is not enabled, select the copy from the table and click **Delete**.

Snapshot freeze scripts and thaw scripts for virtual-machine backups

You can use custom scripts to back up a Windows or Linux virtual machine which runs an application that PowerProtect Data Manager does not directly support. These scripts run before and after the snapshot to place the virtual machine and application into a state where you can perform a backup.

NOTE: Use of these scripts is not supported for virtual machines with the Transparent Snapshot Data Mover (TSDM) protection mechanism enabled.

Table 27. Script descriptions and related terms

Script	Related terms		Description
Freeze	Quiesce	Pre-freeze	This script runs before the snapshot initialization to quiesce the virtual machine and place the application in a frozen state. Quiescing ensures that the data within the guest file system is in a consistent state that is appropriate for backups.
Thaw	Unquiesce	Post-thaw	This script runs after the snapshot finalization to unquiesce the virtual machine, thaw the application, and then return the virtual machine to normal operation.

PowerProtect Data Manager uses the VMware Tools package to quiesce the virtual machine. The [VMware documentation](#) provides more information. Before you deploy the freeze and thaw scripts, install the latest version of the VMware Tools package on the virtual machine.

The freeze and thaw scripts are specific to each application. If the freeze script returns a nonzero exit code, snapshot creation fails.

After you create your custom scripts, deploy the scripts to the correct location on the virtual machine, as specified in the following tables.

Table 28. Script locations for Windows virtual machines

ESXi version	Freeze script location	Thaw script location
ESXi 6.5 or later	C:\Program Files\VMware\VMware Tools\backupScripts.d\ All scripts are invoked in ascending alphabetical order with <code>freeze</code> as the first argument.	C:\Program Files\VMware\VMware Tools\backupScripts.d\ All scripts are invoked in descending alphabetical order with <code>thaw</code> or <code>freezeFail</code> as the first argument.

Table 29. Script locations for Linux virtual machines

ESXi version	Freeze script location	Thaw script location
ESXi 6.5 or later	/usr/sbin/pre-freeze-script	/usr/sbin/post-thaw-script

For Linux virtual machines, set the script ownership and permissions after you deploy the scripts:

- `sudo chown root:root /usr/sbin/pre-freeze-script /usr/sbin/post-thaw-script`
- `sudo chmod 0700 /usr/sbin/pre-freeze-script /usr/sbin/post-thaw-script`

Add a Cloud Tier schedule to a protection policy

For some protection policy types, you can add a Cloud Tier schedule to a protection policy in order to perform backups to Cloud Tier.

Prerequisites

Ensure that a protection storage system is set up for Cloud Tiering.

About this task

You can create the Cloud Tier schedule from **Primary Backup**, **Replicate**, and **Extend Retention** stages. Schedules must have a retention time of 14 days or more.

Cloud Tiering happens at 00:00 UTC each day. Depending on your time zone, this time may be within business hours and thus Cloud Tiering may impact available network bandwidth. Cloud Tiering applies to both centralized and self-service protection policies.

Steps


1. Log in to the PowerProtect Data Manager user interface as a user with the Administrator role.
2. From the PowerProtect Data Manager UI, select **Protection > Protection Policies**, and then click **Add**. The **Add Policy** wizard appears.
3. On the **Type** page, enter a name and description, select the type of system to back up, and click **Next**.

The following protection policy types support Cloud Tiering:

- Virtual machine
- SQL
- Exchange
- Oracle
- SAP HANA
- File System

- Kubernetes

4. On the **Purpose** page, select from the available options to indicate the purpose of the new protection policy, and then click **Next**.
5. On the **Assets** page, select the assets that you want to protect with this policy, and then click **Next**.
6. On the **Objectives** page, click **Add** under **Primary Backup** if the primary backup schedule is not already created, and fill out the fields in the Target and Schedules panes on the **Add Primary Backup** dialog.

 **NOTE:** There is no minimum recurrence required for the Cloud stage, however, the Cloud Tier schedule requires a minimum retention period of 14 days in the **Retain for** field.

7. Click **Cloud Tier** next to **Primary Backup** or **Extend Retention** or, if adding a Cloud stage for a replication schedule that you have added, click **Cloud Tier** under **Replicate**.
An entry for **Cloud Tier** is created to the right of the primary backup or extended retention schedule, or below the replication schedule.
8. Under the entry for **Cloud Tier**, click **Add**.
The **Add Cloud Tier Backup** dialog appears, with summary schedule information for the parent node. This information indicates whether you are adding this Cloud Tier stage for the primary backup schedule, the extended retention schedule, or the replication schedule.
9. In the **Add Cloud Tier Backup** dialog box, set the following parameters and then click **Save**:
 - Select the appropriate storage unit from the **Cloud Target** list.
 - For **Tier After**, set a time of 14 days or more.

The protection policy schedule is now enabled with Cloud Tiering.

10. Click **Next** to proceed with the remaining pages of the **Add Policy** wizard, verify the information, and then click **Finish**.
A new job is created, which you can view under the **Jobs** tab after the job completes.


Manage Cloud Tier asset copies

You can manage Cloud Tier copies of assets by changing copy retention time, deleting copies, and recalling copies.

Steps

1. From the PowerProtect Data Manager UI, select **Infrastructure > Assets**.
2. Select an asset and click **View Copies**.
3. Click an asset copy icon.
Cloud Tier backups are listed by cloud storage in the **Location** column.
4. To change how long copies remain in cloud storage, complete the following steps:
 - a. Select a Cloud Tier backup and click **Edit Retention**.
 - b. Choose one of the following options:
 - To select a calendar date as the expiration date for backups, select **Retention Date**.
 - To define a fixed retention period in days, weeks, months, or years after the backup is performed, select **Retention Value**. For example, you could specify that backups expire after 6 months.
 - c. When satisfied with the changes, click **Save**.


The asset is displayed in the list with the changes. The **Retention** column displays both the original and new retention period, and indicates whether the retention period has been extended or shortened.

 **NOTE:** When you edit the retention period for copies that are retention locked, you can only extend the retention period.

5. To delete the copy in cloud storage, select a Cloud Tier backup and click **Delete**. To delete the copy records from the PowerProtect Data Manager database while the copy remains in the protection storage, select **Remove from PowerProtect**.

[Delete backup copies](#) on page 95 and [Remove backup copies from the PowerProtect Data Manager database](#) on page 97 provides more information.

6. Select a Cloud Tier backup and click **Recall from Cloud** to return the cloud backup to your local protection storage for recovery or backup.

 **NOTE:** If you use Amazon's network to copy data from AWS storage, Amazon charges you for the data transfer.

7. To extend the date to retier the copy back to the cloud, select **Edit Recall Retention**.

8. To manually move a copy back to cloud storage, select **Retier**.

Manual backups of protected assets

Once assets have been added to a protection policy, you can perform manual backups by using the **Protect Now** functionality in the PowerProtect Data Manager UI.

You can use a single manual backup from the **Protection > Protection Policies** window to back up multiple assets that are protected in the designated protection policy. To perform this manual backup:

1. From the PowerProtect Data Manager UI, select **Protection > Protection Policies**
2. Select the protection policy that contains the assets that you want to back up, and click **Protect Now**.

The **Protect Now** wizard appears.

NOTE: The protection policy must be enabled, and its purpose must not be Exclusion or Self-Service Protection.

3. On the **Assets Selection** page, select whether you want to back up all assets or choose individual assets that are defined in the protection policy, and then click **Next**.
4. If you selected the option to choose individual assets for manual backup instead of all assets, the **Assets** page appears with the individual assets available for selection. Select the assets that you want to include in the manual backup, and then click **Next** to display the **Configuration** page.

If you selected to back up all assets, the **Configuration** page appears.

5. On the **Configuration** page, select **Back up now**, and then select from the available backup types.
6. Edit the retention period if you want to change the default settings, and then click **Next**.

The default settings are inherited from the primary backup stage of the parent protection policy.

7. On the **Summary** page, review the settings and then click **Protect Now**. A notification appears indicating whether the request was processed successfully.

You can also perform a manual backup from the **Infrastructure > Assets** window, but only for one asset at a time. To perform this manual backup:

1. From the PowerProtect Data Manager UI, select **Infrastructure > Assets**.
 2. Select the tab for the asset type you want to back up. A list of assets appears.
 3. Select an asset from the table that has an associated protection policy.
- NOTE:** You can select only one asset at a time for manual backup. The protection policy must be enabled, and its purpose must not be Exclusion or Self-Service Protection. A full backup is created for the selected asset.
4. Click **Protect Now**. A notification appears indicating whether the request was processed successfully.

When a virtual machine is part of an application-aware protection policy, the manual backup is a full application-aware backup.

NOTE: The manual backup is managed by other configured stages (extended retention backup, replication, Cloud Tier, Cloud DR) of the parent protection policy.

Manual replication of protected assets

You can perform replication of one more protected assets within a protection policy by using the **Protect Now** functionality in the PowerProtect Data Manager UI.

NOTE: VMAX storage groups only support MTree replication, which is performed and scheduled from the DD system. Therefore, manual replication for assets in a VMAX storage group is not supported.

To perform manual replication:

1. From the PowerProtect Data Manager UI, select **Protection > Protection Policies**
2. Select the protection policy that contains the assets that you want to replicate, and click **Protect Now**.

The **Protect Now** wizard appears.


NOTE: The protection policy must be enabled, its purpose must not be Exclusion, and the policy must already be configured with a replication stage.

3. On the **Assets Selection** page, select whether you want to replicate all assets or choose individual assets that are defined in the protection policy, and then click **Next**.

4. If you selected the option to choose individual assets for manual replication instead of all assets, the **Assets** page appears with the individual assets available for selection. Select the assets that you want to include in the manual replication, and then click **Next** to display the **Configuration** page.

If you selected to replicate all assets, the **Configuration** page appears.

5. On the **Configuration** page, select **Replicate now**, and then select from the available replication stages.

 **NOTE:** Only replication stages for the primary backup are available for selection.


6. Edit the retention period if you want to change the default settings, and then click **Next**.

The default settings are inherited from the primary backup stage of the parent protection policy.


7. On the **Summary** page, review the settings and then click **Protect Now**. A notification appears indicating whether the request was processed successfully.

Manual Cloud Tiering of protected assets

Once you add assets to a protection policy that contains a Cloud Tier stage, you can perform a manual tiering of these assets by using the PowerProtect Data Manager UI.

 **NOTE:** Manual Cloud Tiering of a copy set requires the related protection policy to have a Cloud Tier stage.

To perform on-demand Cloud Tiering:

1. From the PowerProtect Data Manager UI, select **Infrastructure > Assets**.
 2. On the **Assets** window, select the tab for the asset type you want to tier. A list of assets appears.
 3. Select an asset from the table that has an associated protection policy, and then click **View Copies**.
-  **NOTE:** You can only select one asset at a time, and the protection policy that is associated with the asset cannot be an exclusion policy.
4. Click the **DD** icon to display the available backup copies in the right pane.
 5. Select a backup copy, and then click **Tier**. A notification appears indicating whether the request was processed successfully.


Go to the **Jobs** window to monitor the progress of the tiering operation.

Editing a protection policy

You can use the PowerProtect Data Manager UI to change any of the following information for an existing enabled or disabled protection policy:

- Policy name and description
- Backup schedule
- Backup optimization mode
- Settings for network interface, storage quotas, and retention lock
- Adding or removing assets from the policy.

You cannot modify a protection policy type or purpose. For these actions, add a policy.

 **NOTE:** Once you save changes for an enabled or disabled policy, most changes take effect immediately. For a disabled policy's primary backup schedules, however, the changes do not take effect until you reenable the policy, since these schedules do not run in **Disabled** state.

Modify a policy name and description, objectives, or options

The following procedure describes how to change an existing policy name and description, schedule and objectives, or additional backup options in the PowerProtect Data Manager UI.

Prerequisites

If applicable, complete all of the virtual network configuration tasks before you assign any virtual networks to the protection policy.

About this task

NOTE: You can also edit a protection policy to add or remove assets. Detailed instructions for adding assets to a policy or removing assets from a policy are provided in the section [Add or remove assets in a protection policy](#) on page 91.

Steps

1. From the left navigation pane, select **Protection > Protection Policies**.
The **Protection Policies** window appears.
2. Select the protection policy that you want to modify, and click **Edit**.
The **Edit Policy** window opens on the **Summary** page. From this page, you can click edit next to any available row to change specific policy details.
3. In the **Name** or **Description** rows, click **Edit**.
The **Type** page displays.
NOTE: You cannot change the type or purpose of an existing policy.
4. In the **Objectives** row, click **Edit**.
The **Objectives** page displays. From this page, you can change the backup schedule, modify the settings for the network interface, and enable or disable the retention lock.
NOTE: Dell Technologies recommends that you do not edit the network interface for application agent assets such as File System, SQL, ORACLE, and SAP HANA, because modifying this setting causes subsequent backup failure. As a workaround, set the lockbox, which initiates a new asset configuration.

You can also change the storage targets by selecting a new **Storage Name** in the **Primary Backup** and **Replicate** rows. For more information about changing storage targets, see the section [Changing storage targets and storage units](#) on page 90.
5. In the **Options** row, click **Edit**.
The **Options** page displays. From this page, you can change the backup optimization mode (for example, from Performance to Capacity), select whether to include or exclude swap files from the backup, and select whether to quiesce the guest file system during the backup.
NOTE: For virtual machine protection policies, two types of protection mechanisms are used—Transparent Snapshot Data Mover (TSDM), and VMware vStorage API for Data Protection (VADP). Updates to the policy options can result in changes to the protection mechanism used to move virtual machine data. When the protection mechanism changes, a new, full backup is performed, which might take awhile to complete.
6. After making your changes, click **Next** to save the changes and return to the **Summary** page.
7. On the **Summary** page, click **Finish**.
An informational dialog displays.
8. 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.

Changing storage targets and storage units

You can change the storage target or storage unit that PowerProtect Data Manager targets for each protection policy.

When editing protection policies in the PowerProtect Data Manager UI, for the **Primary Backup** and **Replicate** schedules on the **Objectives** page:

- The **Storage Name** drop-down list shows the current storage target and those storage targets that are available for the protection policy.
- The **New** and **Existing** options for **Storage Unit** show the current storage unit that PowerProtect Data Manager targets on the selected protection storage system.

Storage targets

When reviewing the list of selected and available storage targets, consider the following:

- The selected storage target for **Storage Name** in the **Primary Backup** row does not appear in the drop-down list for **Storage Name** in the **Replicate** row.
- The selected storage target for **Storage Name** in the **Replicate** row does not appear in the drop-down list for **Storage Name** in the **Primary Backup** row.

- Only those storage targets that have been licensed and configured for use by the current protection policy appear in a drop-down list.
- If a storage target exists but does not appear in a drop-down list, click **Add** at the bottom of the list. Configure the storage target for use with the protection policy.
- When a storage target is changed, a new `storage unit name` is automatically created, and the configuration is passed to any backup agents.
- Changing storage targets in Storage Group protection policies is not supported.

NOTE:

Changing the storage target for **Primary Backup** may prevent any scheduled backups from being performed until after the next full backup. To ensure that all scheduled backups are performed on schedule, click **Back Up Now** from the **Protection > Protection Policies** pane.

This guidance does not apply to VMware crash-consistent or file system backups for **Primary Backup**. For those asset types, you can change the storage target and all scheduled backups happen without further action. This guidance also does not apply to replication.

When you change a storage target, appropriately configure any dependencies. For example, configuring a cloud provider to use the new storage target.

Storage units

[Storage units](#) on page 40 provides more information about working with storage units, including applicable limitations and maintenance considerations.

When you select **New**, PowerProtect Data Manager maintains a dedicated storage unit for this protection policy. Click **Set Storage Quotas**.

Set the capacity and stream quotas that restrict the storage unit resource consumption.

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. When you set a hard limit and the limit is reached, data cannot be written. All data protection operations fail until data is deleted from the storage unit. The *PowerProtect DD Virtual Edition Installation and Administration Guide* for the appropriate platform provides more information about quota configuration.

- **Capacity Quota**—Controls the total size of precompression data that is written to the protection storage.
- **Stream Quota**—The number of concurrent streams allowed during data protection operations. Setting a **Stream Quota** limit can help ensure that performance is not impacted negatively when a data protection operation consumes too many resources.

When you select **Existing**, the protection policy targets a storage unit under the control of PowerProtect Data Manager. Click **Select**.

The **Select Storage Unit** dialog box opens and displays a list of the storage units under the control of PowerProtect Data Manager.

Select a storage unit from the list, and then click **Select**.

Add or remove assets in a protection policy

Perform the following steps in 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.

Steps

1. From the left navigation pane, select **Protection > Protection Policies**.
The **Protection Policies** 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.

NOTE: For virtual machine protection policies, the view that you selected when creating the policy is retained in this page, and cannot be changed. For example, if you set up this policy with **View Asset Table** selected, all assets protected by this policy will display in a table on this page, and the option to select **View by Host** will be disabled. Both views provide additional information about the virtual machines, such as any currently associated tags, protection rules, and whether the virtual machine is already assigned to another policy, to help you identify which assets you want to add or remove from this policy.

4. To remove containers or assets from the protection policy, select the object and click **Remove**.

The **Assets** page updates with the changes.

5. To add a container or asset to the protection policy:

- a. Click **+ Add**.

The **Add Unprotected Assets** dialog displays any objects that are unprotected.

- b. Select the individual unprotected assets that you want to add to the policy, or select a container level within the hierarchy to add all assets within that level, and then click **Add**.

The **Assets** page updates with the changes.

6. Optionally, if you want to exclude non-production VMDKs such as network shares or test disks from a protection policy:

- a. Select the virtual machine asset from the list, and then click **Manage Exclusions** in the **Disk Excluded** column.

The **Exclude Disks** dialog box appears. By default, the slider next to each VMDK is set to **Included**.

- b. For each disk that you want to exclude, move the slider to the right. The status updates to **Excluded**.

NOTE: For PowerProtect Data Manager version 19.3, a virtual machine with disk exclusion and Cloud Disaster Recovery (DR) cannot coexist in the same protection policy. If you exclude disks from a virtual machine protection policy, Cloud DR is not supported.

- c. Click **Save**. The **Assets** page updates to indicate the number of disks for that particular asset that will be excluded from the protection policy.

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.

View assets assigned to a protection policy

You can view assets that are assigned to a protection policy. If the modification of a protection rule results in assets moving from one protection policy to another, you can verify the results from the details window for the protection policy.

About this task

To view the assets that are assigned to a protection policy, complete the following steps:

Steps

1. From the left navigation pane, select **Protection > Protection Policies**.

The **Protection Policies** window opens.

2. Click the name of the protection policy to view its details.

The details window for the selected protection policy opens and displays information about the policy.

3. Click the asset count link next to **Assets**.

The **Assets** window appears and displays the assets that are assigned to the protection policy.

Extended retention

You can extend the retention period for the primary backup copy for long term retention. For example, your regular schedule for daily backups can use a retention period of 30 days, but you can extend the retention period to keep the full backups taken on Mondays for 10 weeks.

Both centralized and self-service protection policies support weekly, monthly, and yearly recurrence schedules to meet the demands of your compliance objectives. For example, you can retain the last full backup containing the last transaction of a fiscal year for 10 years. When you extend the retention period of a backup in a protection policy, you can retain scheduled full backups with a repeating pattern for a specified amount of time.

For example:

- Retain full yearly backups that are set to repeat on the first day of January for 5 years.
- Retain full monthly backups that are set to repeat on the last day of every month for 1 year.
- Retain full yearly backups that are set to repeat on the third Monday of December for 7 years.

Preferred alternatives

When you define an extended retention stage for a protection policy, you define a set of matching criteria that select preferred backups to retain. If the matching criteria do not identify a matching backup, PowerProtect Data Manager automatically retains the preferred alternative backup according to one of the following methods:

- Look-back—Retain the last available full backup that was taken before the matching criteria.
- Look-forward—Retain the next available full backup that was taken after the matching criteria.

For example, consider a situation where you configured a protection policy to retain the daily backup for the last day of the month to extended retention. However, a network issue caused that backup to fail. In this case, look-back matching retains the backup that was taken the previous day, while look-forward matching retains the backup that was taken the following day.

By default, PowerProtect Data Manager uses look-back matching to select the preferred alternative backup. A grace period defines how far PowerProtect Data Manager can look in the configured direction for an alternative backup. If PowerProtect Data Manager cannot find an alternative backup within the grace period, extended retention fails.

You can use the REST API to change the matching method or the grace period for look-forward matching. The [PowerProtect Data Manager Public REST API documentation](#) provides instructions. If there are no available backups for the defined matching period, you can change the matching method to a different backup.

For look-forward matching, the next available backup can be an ad-hoc backup or the next scheduled backup.

Selecting backups by weekday

This section applies to centralized protection policies. Self-service protection policies have no primary backup schedule configuration.

When you configure extended retention to match backups by weekday, PowerProtect Data Manager may identify a backup that was taken on one weekday as being taken on a different weekday. This behavior happens where the backup window does not align with the start of the day. PowerProtect Data Manager identifies backups according to the day on which the corresponding backup window started, rather than the start of the backup itself.

For example, consider a backup schedule with an 8:00 p.m. to 6:00 a.m. backup window:

- Backups that start at 12:00 a.m. on Sunday and that end at 6:00 a.m. on Sunday are identified as Saturday backups, since the backup window started on Saturday.
- Backups that start at 8:01 p.m. on Sunday and that end at 12:00 a.m. on Monday are identified as Sunday backups, since the backup window started on Sunday.
- Backups that start at 12:00 a.m. on Monday and that end at 6:00 a.m. on Monday are identified as Sunday backups, since the backup window started on Sunday.

In this example, when you select Sunday backups for extended retention, PowerProtect Data Manager does not retain backups that were taken between 12:00 a.m. and 8:00 p.m. This behavior happens even though the backups occurred on Sunday. Instead, PowerProtect Data Manager selects the first available backup that started after 8:00 p.m. on Sunday for extended retention.

If no backups were created between 8:01 p.m. on Sunday and 6:00 a.m. on Monday, PowerProtect Data Manager retains the next alternative to extended retention. In this example, the alternative was taken after 6:00 a.m. on Monday.

Extended retention backup behavior

When PowerProtect Data Manager identifies a matching backup, automatic extended retention creates a job at the beginning of the backup window for the primary stage. This job remains queued until the end of the backup window and then starts.

The following examples describe the behavior of backups with extended retention for centralized and self-service protection.

Centralized protection

For an hourly primary backup schedule that starts on Sunday at 8:00 p.m. and ends on Monday at 6:00 p.m. with a weekly extended retention schedule that is set to repeat every Sunday, PowerProtect Data Manager selects the first available backup starting after 8:00 p.m. on Sunday for long-term retention.

The following diagram illustrates the behavior of backups with extended retention for a configured protection policy. In this example, full daily backups starting at 10:00 p.m. and ending at 6:00 a.m. are kept for 1 week. Full weekly backups are set to repeat every Sunday and are kept for 1 month.

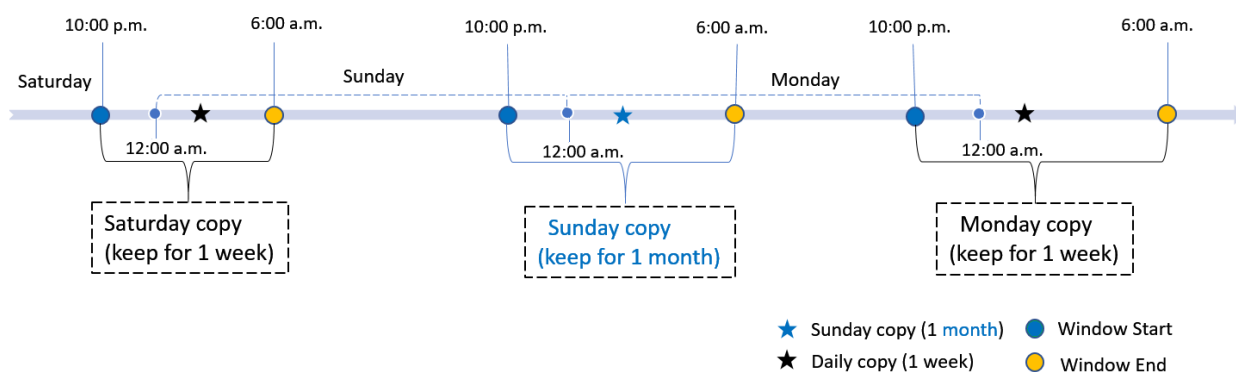


Figure 2. Extend retention backup behavior

Self-service protection

For self-service backups, PowerProtect Data Manager uses a default backup window of 24 hours. For a backup schedule that starts on Sunday at 12:00 p.m. and ends on Monday at 12:00 p.m. with a weekly extended retention schedule that is set to repeat every Sunday, PowerProtect Data Manager selects the first available backup that is taken between 12:00 p.m. on Sunday and 12:00 p.m. on Monday for long-term retention.

Edit the retention period for backup copies

You can edit the retention period of one or more backup copies to extend or shorten the amount of time that backups are retained.


About this task

You can edit retention for all asset types and backup types.

Steps

1. From the PowerProtect Data Manager UI, select **Infrastructure > Assets**.
2. On the **Assets** window, select the tab for the asset type for which you want to edit retention. If a policy has been assigned, the table lists the assets that have been discovered, along with the associated protection policy.

NOTE: For virtual-machine assets, you can click the link in the **Disk Excluded** column next to a virtual-machine asset to view VMDKs that have been excluded from the protection policy. You cannot, however, edit disk inclusion or exclusion from this window. To change the disks that are excluded for a protected asset, select the policy from the **Protection Policies** window and click **Edit**.

3. Select a protected asset from the table, and then click **View Copies**. The **Copy Locations** pane identifies where the backups are stored.
 4. In the left pane, click the storage icon to the right of the icon for the asset, for example, **DD**. The table in the right pane lists the backup copies.
 5. Select one or more backup copies from the table and click **Edit Retention**.
 6. Choose one of the following options:
 - To select a calendar date as the expiration date for backups, select **Retention Date**.
 - To define a fixed retention period in days, weeks, months, or years after the backup is performed, select **Retention Value**. For example, you could specify that backups expire after 6 months.
-  **NOTE:** When you edit the retention period for copies that are retention locked, you can only extend the retention period.
7. When satisfied with the changes, click **Save**.
The asset is displayed in the list with the changes. The **Retention** column displays both the original and new retention period, and indicates whether the retention period has been extended or shortened.

Delete backup copies

In addition to deleting backups upon expiration of the retention period, PowerProtect Data Manager enables you to manually delete backup copies from protection storage.

About this task


If you no longer require a backup copy and the retention lock is not enabled, you can delete backup copies prior to their expiration date.

You can perform a backup copy deletion that deletes only a specified part of a backup copy chain, without impacting the ability to restore other backup copies in the chain. When you select a specific backup copy for deletion, only that backup copy and the backup copies that depend on the selected backup copy are deleted. For example, when you select to delete a full backup copy, any other backup copies that depend on the full backup copy are also deleted.


Steps

1. From the PowerProtect Data Manager UI, select **Infrastructure > Assets**.
2. From the **Assets** window, select the tab for the asset type for which you want to delete copies. If a policy has been assigned, the table lists the assets that have been discovered, along with the associated protection policy.
3. Select a protected asset from the table, and then click **View Copies**. The **Copy Locations** pane identifies where the backups are stored.
4. In the left pane, click the storage icon to the right of the icon for the asset, for example, **DD**. The table in the right pane lists the backup copies.
5. Select one or more copies from the table that you want to delete from the DD system, and then click **Delete**.

A preview window opens and displays the selected backup copies.

 **NOTE:** For assets with backup copies that are chained together such as Microsoft SQL databases, Oracle databases, SAP HANA databases, and application-aware virtual machines, the preview window lists all the backup copies that depend on the specified backup copy. If you delete a backup copy, PowerProtect Data Manager deletes the specified backup copy and all backup copies that depend on the specified backup copy.

6. For all asset types, you can choose to keep the latest backup copies or delete them. By default, PowerProtect Data Manager keeps the latest backup copies. To delete the latest backup copies, clear the checkbox next to **Include latest copies**.
For VMAX storage group backup copies, you can choose to delete copies that are grouped together in the same protection transaction or delete only selected copies. By default, PowerProtect Data Manager deletes copies that are grouped together in the same protection transaction. To delete only selected copies, clear the checkbox next to **Include copies in the same protection transaction**.
7. To delete the backup copies, in the preview window, click **Delete**.

 **NOTE:** The delete operation may take a few minutes and cannot be undone.

An informational dialog box opens to confirm the copies are being deleted. To monitor the progress of the operation, click **Go to Jobs**. To view the list of backup copies and their status, click **OK**.

When the job completes, the task summary provides details of each deleted backup copy, including the time that each copy was created, the backup level, and the retention time. The time of copy creation and the retention time is shown in UTC.

An audit log is also generated and provides details of each deleted backup copy, including the time that each copy was created, the backup level, and the retention time. The time of copy creation and the retention time is shown in UTC. Go to **Alerts > Audit Logs** to view the audit log.

8. Verify that the copies are deleted successfully from protection storage. If the deletion is successful, the deleted copies no longer appear in the table.

Retry a failed backup copy deletion

If a backup copy is not deleted successfully, you can manually retry the operation.

Steps

1. From the PowerProtect Data Manager UI, select **Infrastructure > Assets**.
2. From the **Assets** window, select the tab for the asset type for which you want to delete copies. If a policy has been assigned, the table lists the assets that have been discovered, along with the associated protection policy.
3. Select a protected asset from the table, and then click **View Copies**. The **Copy Locations** pane identifies where the backups are stored.
4. In the left pane, click the storage icon to the right of the icon for the asset, for example, **DD**. The table in the right pane lists the backup copies.
5. Select one or more backup copies with the **Deletion Failed** status from the table, and then click **Delete**.
You can also filter and sort the list of backup copies by status in the **Copy Status** column.
The system displays a warning to confirm you want to delete the selected backup copies.
6. Click **OK**.
An informational dialog box opens to confirm that the copies are being deleted. To monitor the progress of the operation, click **Go to Jobs**. To view the list of backup copies and their status, click **OK**.
7. Verify that the copies are successfully deleted from protection storage. If the deletion is successful, the deleted copies no longer appear in the table.


Export data for deleted backup copies

This option enables you to export results of deleted backup copies to a CSV file so that you can download an Excel file of the data.

Steps

1. From the PowerProtect Data Manager UI, select **Infrastructure > Assets**.
2. From the **Assets** window, select the tab for the asset type for which you want to export results of deleted backup copies. If a policy has been assigned, the table lists the assets that have been discovered, along with the associated protection policy.
3. Select one or more protected assets from the table and then select **More Actions > Export Deleted Copies**.
If you do not select an asset, PowerProtect Data Manager exports the data for deleted backup copies for all assets for the specific asset type.
4. Specify the following fields for the export:
 - a. **Time Range**
The default is **Last 24 Hours**.
 - b. **Copy Status**
In order to export data for deleted backup copies, the backup copies must be in one of the following states:
 - **Deleted**—The copy is deleted successfully from protection storage, and, if applicable, the agent catalog is deleted successfully from the agent host.
 - **Deleting**—Copy deletion is in progress.
 - **Deletion Failed**—Copy deletion from protection storage is unsuccessful.
 - **Deletion Failed (Agent Catalog)**—The copy is deleted successfully from protection storage, but is not deleted from the agent host.

 **NOTE:** This state is not applicable to virtual machine and Kubernetes backup copies.

 **NOTE:** You cannot export data for backup copies that are in an **Available** state.

5. Click **Download**.
If applicable, the navigation window appears for you to select the location to save the CSV file.
6. Save the CSV file in the desired location and click **Save**.

Remove backup copies from the PowerProtect Data Manager database

This option enables you to delete the backup copy records from the PowerProtect Data Manager database, but keep the backup copies in protection storage.

About this task

For backup copies that could not be deleted from protection storage, you can remove the backup copies from the PowerProtect Data Manager database. Removing the backup copies from PowerProtect Data Manager does not delete the copies in protection storage.

Steps

1. From the PowerProtect Data Manager UI, select **Infrastructure > Assets**.
2. From the **Assets** window, select the tab for the asset type for which you want to delete copies. If a policy has been assigned, the table lists the assets that have been discovered, along with the associated protection policy.
3. Select a protected asset from the table, and then click **View Copies**. The **Copy Locations** pane identifies where the backups are stored.
4. In the left pane, click the storage icon to the right of the icon for the asset, for example, **DD**. The table in the right pane lists the backup copies.
5. Select one or more backup copies with the **Deletion Failed** or **Deletion Failed (Agent Catalog)** status from the table, and then click **Remove from PowerProtect**.

For backup copies with the **Deletion Failed (Agent Catalog)** status, click **Remove from PowerProtect** to remove the information from PowerProtect Data Manager for any backup copies that were successfully deleted from protection storage but for which the agent catalog was not deleted from the agent host.

The system displays a warning to confirm you want to delete the selected backup copies.

6. Click **OK**.
An informational dialog box opens to confirm that the copies are being deleted. To monitor the progress of the operation, click **Go to Jobs**. To view the list of backup copies and their status, click **OK**.
7. Verify that the copies are deleted from the PowerProtect Data Manager database. If the deletion is successful, the deleted copies no longer appear in the table. The backup copies remain in protection storage.

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 specifying retention periods for a protection policy schedule is provided within the topic for each policy type.

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:

- **Exclusion** – The asset is currently assigned to an exclusion protection policy.
- **Disabled** – The asset is currently assigned to a disabled protection policy.
- **Protected** – The asset is currently assigned to an enabled protection policy.
- **Previously Protected** – The asset has been unassigned from a protection policy and has not yet been re-assigned to another policy or assigned to an Exclusion policy.

For an asset assigned to either an exclusion or disabled protection policy, PowerProtect Data Manager deletes the expired backup copies for the asset when the following settings are set to **true**:

- `expiredCopyDeletionEnabledForAssetInExclusionPolicy`
- `expiredCopyDeletionEnabledForAssetInDisabledPolicy`

The expired copy deletion settings for exclusion and disabled protection policies are set to **true** by default. If either setting is set to **false**, PowerProtect Data Manager skips deletion of the expired backup copies. The [PowerProtect Data Manager Public REST API documentation](#) provides more information.

Expired copy cleanup occurs at 00:00 AM UTC each day. If a copy deletion fails, a warning alert appears in the audit log under **Alerts > System**.


You can monitor the progress of the expired copy removal job from the **Jobs** window.

Removing assets from PowerProtect Data Manager

PowerProtect Data Manager automatically removes assets if certain conditions are met. However, some assets can be manually removed.

Assets are automatically removed if the following conditions are met:

- The status of the asset is **Deleted**.
- The asset has no backup copies.
- The asset has existed for longer than the value of the asset TTL setting. This is 0 minutes by default, but it can be changed with the REST API. For more information, see [PowerProtect Data Manager Public REST API documentation](#).

 **NOTE:** This value has changed from earlier versions of PowerProtect Data Manager.

The manual removal of assets allows for the following increased control over the process:

- The asset can be removed on demand.
- The status of the asset can be **Not Detected**.
- All protection copies of the asset, including replicated and cloud tiered copies, can be manually removed, followed by the manual removal of the asset.
- All protection copies of the asset can be automatically removed, if this option is selected during manual asset removal from PowerProtect Data Manager,

Remove assets and associated protection copies

In the PowerProtect Data Manager UI, you can manually remove some assets ahead of their scheduled removal, or remove assets that have not been automatically removed.

Prerequisites


- The asset has a status of **Deleted** or **Not Detected**.
- The asset has no protection copies. If copies still exist in the storage system for the asset, you can delete these copies before following the steps in this procedure or select an option to automatically delete the copies when the asset is removed. For information on deleting backup copies, see [Delete backup copies](#) on page 95.

Steps

1. Select **Infrastructure > Assets**.
2. Select the tab that corresponds to the type of assets that you want to remove. For example, for vCenter virtual machine assets, click **Virtual Machine**.

Assets that are associated with protection copies of this type are listed. By default, only assets with **Available** or **Not Detected** status display. You can also search for assets by name.

3. Select one or more assets from the list, and then click **More Actions > Remove Asset**. The **Remove Assets** dialog displays.
4. Select from one of the following options:

 **NOTE:** All of these options might not display for the selected assets. The available options depend upon the protection copy status of the selected assets.

- **Remove assets and associated protection copies**—removes these assets from PowerProtect Data Manager, and automatically removes any protection copies for these assets from storage.
- **Only remove assets with no associated protection copies**—these assets will not be deleted if PowerProtect Data Manager detects that protection copies for these assets still exist in the storage system.

- **Mark "Not Detected" assets as "Deleted" but keep associated protection copies**—mark assets with **Not Detected** status as **Deleted** in the PowerProtect Data Manager UI, but retain protection copies for these assets in the storage system. You can view assets marked as **Deleted** from the **Infrastructure > Assets** pane.

5. Click **OK** to confirm the asset removal.

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.

Steps

1. From the PowerProtect Data Manager UI, select **Protection > Protection Policies**.

The **Protection Policies** 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**.

Disable a protection policy

From the PowerProtect Data Manager UI, you can disable a protection policy to temporarily stop running certain backup schedules of this policy.

About this task

There are several reasons why you might want to disable a protection policy. For example, by disabling a policy, you can:

- Edit the policy and determine the impact of your changes before these changes take effect.
- Stop backup activity on primary storage if the storage is in maintenance or is temporarily unavailable (for example, during a storage upgrade).

By default, disabling a centralized protection policy stops the primary backup schedules of this policy, including synthetic full schedules, full schedules, and so on. Any replication, cloud tier, and extended retention schedules, however, continue to run while the policy is disabled. You can also perform manual primary backups of a policy that is in **Disabled** state by using the **Protect Now** functionality in the PowerProtect Data Manager UI. [Protection jobs running for a disabled policy](#) on page 100 provides information about jobs that continue to run when a policy is disabled.

You can modify the default behavior to make changes regarding which jobs continue to run when a policy is disabled by using System Level overwrites in the REST API. The [PowerProtect Data Manager Public REST API documentation](#) provides instructions.

When a protection policy is disabled, you can edit the policy in the same manner that you would edit an enabled policy. The advantage of editing a policy in **Disabled** state is that you can preview the changes before resuming primary backups of the policy. [Editing a protection policy](#) on page 89 provides more information about modifying the details of an existing policy.

Steps

1. From the left navigation pane, select **Protection > Protection Policies**.
The **Protection Policies** window opens.
2. Select one or more policies in **Enabled** state. You can also select the checkbox at the top of the table to select all policies on the current page.
3. Click **Disable**.

Results

The policy status changes to **Disabled**. In **Disabled** state:

- In progress primary backup jobs that are associated with this policy continue to run until complete. If primary backups are scheduled to run during the time that the policy is disabled, those backups do not run, even when you enable the policy again. When you re-enable the policy, future scheduled backups resume.
- All other protection jobs for the policy continue to run according to schedule, unless no primary backup copy exists for the policy. In this case, protection jobs are skipped.
- Manual backups of primary schedules can still be performed.

Protection jobs running for a disabled policy

When a protection policy is disabled, only protection jobs related to the primary backup schedules stop running.

The following table provides information about the types of protection jobs that continue to run when a policy is in **Disabled** state. The column **System level overwrite?** indicates whether the default behavior for this job can be overwritten by using the API command. Note, however, that when a policy is disabled, the setting for at least one of these jobs must remain disabled.


 **NOTE:** If no primary backup copy exists for the disabled policy, other scheduled protection jobs such as replication will display as **Skipped** in the **Protection Jobs** window of the PowerProtect Data Manager UI.

Table 30. Protection jobs running when a policy is disabled

Job category	Purpose	Runs when policy is disabled?	System level overwrite?
Centralized scheduled primary protection	Create a primary backup	No	Yes
Manual backup and replication (Protect Now, Replicate Now)	<ul style="list-style-type: none">• Create a primary backup (Protect Now)• Replicates primary backup (Replicate Now)	Yes	No
Self-service protection	Create a primary backup	Yes	No
Policy and asset configuration	Prepare for protection or copy management jobs	Yes	No
Replication	Copy management (location)	Yes	Yes
Cloud DR	Copy management (location)	Yes	Yes
Extended Retention	Copy management (retention)	Yes	Yes
Cloud Tier	Copy management (location)	Yes	Yes
SLA compliance verification	Copy management (report and alert)	Yes	Yes

Table 30. Protection jobs running when a policy is disabled (continued)

Job category	Purpose	Runs when policy is disabled?	System level overwrite?
Delete expired copy	Copy management (reclaiming space on DD)	Yes	Yes

Enable a disabled protection policy

To reenable a disabled policy, perform the following steps:

Steps

1. From the PowerProtect Data Manager UI, select **Protection > Protection Policies**.
2. Select one or more policies in **Disabled** state. You can also select the checkbox at the top of the table to select all policies on the current page.
3. Click **Enable**.

Results

The status changes to **Enabled**. Primary backups for the reenabled policies resume according to the protection policy schedule.

Customize the default behavior of disabled policies

By default, a protection policy in **Disabled** state prevents the primary backup schedules of this policy from running, but does not stop other protection jobs. You can, however, change the default behavior to also stop other activities, such as replication and cloud tiering, by using the REST API.

The [PowerProtect Data Manager Public REST API documentation](#) provides instructions.

Delete a protection policy

Perform the following steps to delete a protection policy that is not protecting any assets.

Prerequisites

If the policy you want to delete protects assets, you must associate those assets with a different protection policy before you can delete the policy.

Steps

1. From the PowerProtect Data Manager UI, select **Protection > Protection Policies**.
2. Select the policy that you want to delete, and then click **Delete**.

Results

After you delete a policy, clean-up of unnecessary components within protection storage occurs automatically according to schedule. Clean-up includes storage units under the control of PowerProtect Data Manager and the corresponding DD Boost users, according to the rules for storage units.

Add a Service Level Agreement

SLA Compliance 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).


About this task

 **NOTE:** When you create an SLA for Cloud Tier, you can include only full backups in the SLA.

Steps





1. From the PowerProtect Data Manager UI, select **Protection > SLA Compliance**.
The **SLA Compliance** window appears.
2. Click **Add** or, if the assets that you want to apply the SLA to are listed, select these assets and then click **Add**.
The **Add Service Level Agreement** wizard 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.
 - **Extended Retention**. If you choose this type, go to step 6.
 - **Replication**. If you choose this type, go to step 7.
 - **Cloud Tier**. If you choose this type, go to step 8.

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, Replication, and Cloud Tier copies.
 - c. If applicable, select **Maximum Copies**, and specify the number of Backup, Replication, and Cloud Tier copies.
 - d. If applicable, select **Available Location** and select the applicable locations. To add a location, click **Add Location**.
Options include the following:
 - **In**—Include locations of all copies in the SLO locations. Selecting this option does not require every SLO location to have a copy.
 - **Must In**—Include locations of all copies in the SLO locations. Selecting this option requires every SLO location to have at least one copy.
 - **Exclude**—Locations of all copies must be non-SLO locations.
 - e. If applicable, select **Allowed in Cloud through Cloud Tier/Cloud DR**.
 - f. Click **Finish**, and then 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 required** (RPO), and then set the duration. The purpose of an RPO is business continuity planning, and indicates 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 required** to configure as an independent objective in the SLA, or select both **Recovery Point Objective required** and **Compliance Window for copy type**. 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 occurs independent of the Compliance Window.
 - Less than or equal to the Compliance Window duration, in which case RPO validation occurs within the Compliance Window.
 - c. If applicable, select **Compliance Window for copy type**, and then select a schedule level from the list (for example, **All, Full, Cumulative**) and set the duration. **Duration** indicates the amount of time necessary to create the backup copy. Ensure that the **Start Time** and **End Time** of backup copy creation falls within the Compliance Window duration specified.


This window specifies the time during which you 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, select **Retention Time Objective**, and specify the number of Days, Months, Weeks, or Years.
 **NOTE:** For compliance validation to pass, the value set for the **Retention Time Objective** must match the lowest retention value set for the backup levels of this policy's target objectives. For example, if you set the synthetic full backup **Retain For** to 30 days but set the full backup **Retain For** to 60 days, the Retention Time Objective must be set to the lower value, in this case, 30 days.
 - 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 new SLA.
6. If you selected **Extended Retention**, specify the following fields regarding the purpose of the new Extended Retention SLA:
 - a. The **SLA Name**.
 - b. If applicable, select **Recovery Point Objective required** (RPO), and then set the duration. The purpose of an RPO is business continuity planning, and indicates the maximum targeted period in which data (transactions) might be lost from an IT service due to a major incident.
 **NOTE:** By default, the RPO provides a grace period of 1 day for SLA compliance verification. For example, with a weekly extended retention schedule, PowerProtect Data Manager provides 8 days for the RPO to pass the SLA Compliance verification.
 - 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, select **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**.
This window specifies the times that are permissible and during which you can expect the specified activity to occur. 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, select **Retention Time Objective**, and specify the number of Days, Months, Weeks, or Years.
 **NOTE:** For compliance validation to pass, the value set for the **Retention Time Objective** must match the lowest retention value set for the backup levels of this policy's target objectives.
 - 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. If you selected Cloud Tier type SLA, specify the following fields regarding the purpose of the new Cloud Tier SLA:
 - a. The **SLA Name**.
 - b. If applicable, select the **Verify expired copies are deleted** option.
This option is a compliance check to determine if PowerProtect Data Manager is deleting expired copies. This option is disabled by default.
 - c. If applicable, select **Retention Time Objective** and specify the number of Days, Months, Weeks, or Years.
 **NOTE:** For compliance validation to pass, the value set for the **Retention Time Objective** must match the lowest retention value set for the backup levels of this policy's target objectives.
 - d. If applicable, select the **Verify Retention Lock is enabled for all copies** option. This option is disabled by default.
 - e. Click **Finish**.
 9. If the SLA has not already been applied to a protection policy:
 - a. Go to **Protection > Protection Policies**.

- b. Select the policy, and then click **Edit**.
10. In the **Objectives** row of the **Summary** window, click **Edit**.
11. Do one of the following, and then click **Next**:
 - Select the added Policy SLA from the **Set Policy Level SLA** list.
 - Create and add the SLA policy from the **Set Policy Level SLA** list.
 The **Summary** window appears.
12. Click **Finish**.
An informational message appears to confirm that PowerProtect Data Manager has saved the protection policy.
13. 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 a.m. Coordinated Universal Time (UTC). If any objectives are out of compliance, an alert is generated at 2 a.m. UTC. The **Validate** job in the **System Jobs** window indicates the results of the daily compliance check.


For a backup SLA with a required RPO setting that is less than 24 hours, PowerProtect Data Manager performs real-time compliance checks. If you selected **Compliance Window for copy type** and set the backup level to **All**, the real-time compliance check occurs every 15 minutes only within the compliance window. If the backup level is not **All**, or if a compliance window is not specified, the real-time compliance check occurs every 15 minutes without stop.

 **NOTE:** If the backup SLA has a required RPO setting of 24 hours or greater, compliance checks occur daily at 2 a.m. UTC. Real-time compliance checks do not occur for backup SLAs with an RPO setting of 24 hours or greater.

Real-time compliance check behavior

If the interval of time between the most recent backup of the asset and the compliance check is greater than the RPO requirement, then an alert indicates the RPO of the asset is out of compliance. This alert is generated once within an RPO period. If the same backup copy is missed when the next compliance check occurs, no further alerts are generated.

If the interval of time between the most recent backup of the asset and the compliance check is less than the RPO requirement, the RPO of the asset is in compliance.

If multiple assets in a policy are out of compliance at the same time when a compliance check occurs, a single alert is generated and includes information for all assets that are out of compliance in the policy. In the **Alerts** window, the asset count next to the alert summary indicates the number of assets that are out of compliance in the policy.
14. 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.

Steps

1. From the PowerProtect Data Manager UI, 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**.

Protection rules

Protection rules comprise one or more conditions that select matching assets and automatically assign them to a corresponding protection policy. PowerProtect Data Manager applies these rules to assets at discovery time.

When you define a protection rule, note the following requirements:

- Creating protection rules requires at least one existing protection policy.
- An asset can only belong to one protection policy.
- Assets can move from one policy to another policy based on the priorities of the protection rules.
- Virtual machine tags created in the **vSphere Client** can only be applied to a protection rule.
- To ensure the protection of homogeneous assets, the protection rule 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 protection rules are designed to include all the AAG virtual machines.

 **NOTE:** Ensure that Oracle protection rules do not use the DB ID and Oracle SID Name field settings that were supported with versions prior to PowerProtect Data Manager 19.6.

You can manually move an asset into a protection policy and override automatic placement through protection rules. Manual assignment protects the asset through the specified policy but protection rules no longer apply to that asset. To apply protection rules again, remove the asset from the protection policy.

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 that you specify when creating a protection rule.

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 protection rule 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 the vCenter server is 15 minutes. When adding a protection rule and using tags as the asset filter, you must select **VM Tags**.

Add a protection rule

Select a protection policy and then define one or more conditions. Where applicable, create compound rules by linking multiple conditions through logical operators.

About this task

Compound rules enable you to combine multiple selection criteria through AND and OR operators for higher precision. For example, assets in a particular data center with particular tags. Compound rules must have at least one condition.

The **Add Protection Rule** wizard displays compound rules in containers. Grouping rules in the same container represents a logical AND of those rules. Placing rules in separate containers represent a logical OR of those rules. For example, the compound rule (A AND B) OR (C) corresponds to one container with rules A and B, and another container with rule C.

The wizard validates fields as you type. As you define the protection rule, the wizard also displays a count of assets which match the entire protection rule, next to **View Filtered Assets**.

Steps

1. From the PowerProtect Data Manager UI, select **Protection > Protection Rules**.
The **Protection Rules** window appears.
2. Click the tab to select the type of host for which you would like to add the protection rule, and then click **Add**. For example, **Virtual Machines**.
The **Add Protection Rule** wizard opens to the **Select Protection Policy** page.
3. Select the target protection policy for the protection rule and then click **Next**.
The **Asset Rules** page appears.
4. Define the purpose of the protection rule:
 - a. **Name.** For example, **Rules Prod Finance**. The name must be unique.
 - b. **Description.** For example, **Finance department production servers**.
5. Define a protection rule:
 - a. Select an attribute. The available attributes depend on the selected host type and include names (such as `Datacenter Name` or `Host Name`), characteristics (such as asset size), tags (VM tags or namespace labels). The `Power State` attribute enables filtering of virtual machine hosts based on the state of the host (such as `Power On`, `Power Off`, or `Suspended`).
 - b. Select a matching criteria. The available matching criteria depend on the selected attribute:
 - For names, matching criteria include options such as `Begins with`, `Ends with`, `Contains`, `Does not contain`, `Equals`, `Match Regular Expression`, and `Does Not Match Regular Expression`.

The `VM Folder Name` and `VM Resource Pool` attributes support protection for all VM assets and resource pools in the selected folder and its subfolders.
 - For characteristics, matching criteria include options such as `Greater than` or `Less than`.
 - For tags, matching criteria include options such as `Includes`, `Does not include`, `In`, or `Not in`. The `In` and `Not in` criteria support multiple tags.
 - For `Power State`, matching criteria include options such as `Equals` and `Does Not Equal`.
 - Where the available matching criteria includes regular expressions, click **i** for a list of supported operators and effects in a separate dialog box.

NOTE:

Regular expressions for the `VM Folder Name` and `VM Resource Pool` attributes use Google RE2J syntax. The operators and effects on the **Optional** tab of the dialog box are unavailable for these attributes. However, the operators and effects on the **Unsupported** tab are available, as are the standard regular expression predefined character classes. For example, `\d` for a digit.

Regular expressions for all other attributes use Elasticsearch regex syntax. These expressions do not support predefined character classes.

Because predefined character classes are valid for some attributes, the UI does not mark these classes as invalid syntax. This is true even for attributes where such classes are not supported.

- c. Depending on the selected attribute, supply a search phrase to compare against the attribute or select an option from the list.

The wizard displays a count of matching assets beside the rule and enables new **Add Rule** options for compound rules.

For example, a rule with the filters `VM Folder Name`, `Contains`, and **Finance** can match assets belonging to your finance department to the selected protection policy.

6. To define a compound rule:

The wizard only enables some **Add Rule** options after the successful validation of other rules in the same container. For example, rules cannot be empty.


- a. Select a logical operation, and then click the corresponding **Add Rule** option.

The wizard adds a blank rule.


- If you selected **AND**, the new rule appears in the same container.
- If you selected **OR**, the new rule appears in a separate container.

- b. Repeat the previous step to define the new protection rule.


- c. To remove a rule from a compound rule, click  for that rule.

 **NOTE:** The wizard disables  for any rules whose deletion would result in an empty container. To remove these rules, remove the entire container.

The wizard removes the selected rule and any associated **Add Rule** options.

- d. To remove an entire container and any rules within it, click  for that container.

The wizard also removes any associated **Add Rule** options.

- e. To remove all rules, click  **Reset Rules**.

The wizard displays a count of matching assets beside each rule and, for each container, a count of matching assets for all rules in the container.

7. To see a list of unprotected assets which match the protection rule, click **View Matching Assets**.

The **Matching Assets** window opens and displays the details of each matching asset. Verify that the list includes all expected assets, and then click **Done**.

8. If the protection rule and list of matching assets do not meet expectations, adjust the rules accordingly. Alternatively, reset the rules and then build the protection rule again.

9. If the protection rule and list of matching assets meet expectations, click **Next**.

The **Summary** page appears.

10. Review the protection rule details and then click **Finish**.


Results

The new protection rule automatically protects any matching assets.

Manually run a protection rule

PowerProtect Data Manager automatically runs protection rules when new assets are detected or when existing assets are modified. You can also run protection rules manually.

Prerequisites

 **NOTE:** For SQL, Oracle, SAP HANA, and file system asset types, the protection rule runs only on scheduled discovery in PowerProtect Data Manager. Ensure that you schedule discovery for these asset types.

Steps

1. From the PowerProtect Data Manager UI, select **Protection > Protection Rules**.

The **Protection Rules** window appears.

2. Select the required protection rules, and then click **Run**.

PowerProtect Data Manager runs all of the selected protection rules for the current asset type.

Schedule asset discovery

To schedule discovery in the PowerProtect Data Manager UI, complete the following steps:

Steps

1. Select **Infrastructure > Asset Sources**.
2. Select the **App/File System Host** tab.
3. Select the application host, and then click **Discover**.
4. From the **Discovery Schedule** list, select the time of day to initiate the discovery.

Edit or delete a protection rule

You can change the name, description, the rule filters, and the associated protection policy.

Steps

1. Select **Protection > Protection Rules**.
The **Protection Rules** window appears.
2. To edit a protection rule, select the rule and then click **Edit**.
The **Edit Protection Rule** window appears.
 - a. Select a protection policy, and then click **Next**.
 - b. Modify the name, description, or filter rules, and then click **Next**.
[Add a protection rule](#) on page 106 provides more information about working with rules.
 - c. Review the protection rule summary, and then click **Finish**.
3. To delete a protection rule, select the rule and then click **Delete**.
PowerProtect Data Manager removes from protection policies any assets that were added because of this protection rule. PowerProtect Data Manager adds those assets again if you do not update related protection rules.

View assets applied to a protection rule

You can view the assets that are applied to a protection rule from the **Protection Rules** window. If the modification of a protection rule results in assets moving from one policy to another, the **Protection Rules** window enables you to verify the results.

About this task

To view assets that are applied to a protection rule, complete the following steps.

Steps

1. From the left navigation pane, select **Protection > Protection Rules**.
The **Protection Rules** window appears.
2. Click the link in the **Assigned Assets Count** column for the protection rule.
The **Assets List** window appears and displays the matched assets.

Change the priority of an existing protection rule

When multiple protection rules exist, you can define the priority of each rule. Priority determines which rule applies to an asset when that asset matches multiple rules and those rules have conflicting actions.

About this task

For example, if an asset matches several protection rules and each rule specifies a different protection policy, then the rule with the highest priority determines the policy assignment.

Protection rule priorities are integers. Smaller integers represent a higher priority.

Steps

1. Select **Protection > Protection Rules**.
The **Protection Rules** window appears.
2. To change a protection rule's priority, select the rule and then click **Up** or **Down**.
Remember that the smaller integer has the higher priority.

Configure protection rule behavior

You can use the REST API to configure what happens when a protection rule changes.

The [PowerProtect Data Manager Public REST API documentation](#) provides instructions.

NOTE:

If you update from a previous release of PowerProtect Data Manager, the configured behavior for protection rules changes still applies to the current release. For example, in PowerProtect Data Manager 19.4, if you did not configure protection rules through `application.properties` to move assets across policies, then you cannot change the behavior with this method in PowerProtect Data Manager 19.5 or later.

However, if you updated the configuration file to enable protection rules to move assets across policies, then this behavior continues to apply after the update.

Restoring Data and Assets

Topics:

- [View backup copies available for restore](#)
- [Restoring a virtual machine or VMDK](#)
- [Restore an application-aware virtual machine backup](#)
- [Restore the PowerProtect Data Manager server](#)
- [Restore Cloud Tier backups to protection storage](#)

View backup copies available for restore

When a protection policy is successfully backed up, PowerProtect Data Manager displays details such as the name of the storage system containing the asset backup, location, the creation and expiry date, and the size. To view a backup summary:

Steps

1. From the PowerProtect Data Manager UI, select **Infrastructure > Assets** or **Restore > Assets**.
2. Select the tab that corresponds to the type of assets that you want to view. For example, for vCenter virtual machine assets, click **Virtual Machine**.

Assets that are associated with protection copies of this type are listed. By default, only assets with **Available** or **Not Detected** status display. You can also search for assets by name.

For virtual machines, you can also click the **File Search** button to search on specific criteria.

NOTE: In the **Restore > Assets** window, only tabs for asset types supported for recovery within PowerProtect Data Manager display. Supported asset types include the following:

- **Virtual Machines**
- **File System**
- **Storage Group**
- **Kubernetes**

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 appears in the right pane. The child nodes represent storage systems.

When you click a child node, the right pane displays the following information:

- Storage system where the copy is stored.
- The number of copies
- Details of each copy, including the time that each copy was created, the consistency level, the size of the copy, the backup type, the copy status, and the retention time.
- The indexing status of each copy at the time of copy creation:
 - **Success** indicates that all files or disks are successfully indexed.
 - **Partial Success** indicates that only some disks or files are indexed and might return partial results upon file search.
 - **Failed** indicates that all files or disks are not indexed.
 - **In Progress** indicates that the indexing job is in progress.

If indexing has not been configured for a backup copy, or if global expiration has been configured and indexed disks or files have been deleted before the backup copy expiration date, the **File Indexing** column displays **N/A**.

The indexing status updates periodically which enables you to view the latest status.

- For virtual machine backups, a **Disk Excluded** column enables you to view any virtual disks (VMDKs) that were excluded from the backup.

Restoring 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.

PowerProtect Data Manager supports multiple data movers for restoring virtual machines, depending on the restore type and the vSphere capabilities. Restores are performed using one of the following data movers:

- Transparent Snapshot Data Mover—Starting in PowerProtect Data Manager version 19.9, Transparent Snapshot Data Mover (TSDM) is the default protection mechanism that is used for crash-consistent virtual machine policies when vCenter/ESXi version 7.0 U3 and later is installed in the environment. Review the section [Prerequisites to restore a virtual machine](#) on page 112 for specific restore type requirements for TSDM.
- VADP—VMware vStorage API for Data Protection (VADP) is the protection mechanism that is used for application aware virtual machine policies and crash-consistent policies that do not meet the TSDM software requirements. VADP is the only protection mechanism available in PowerProtect Data Manager versions 19.8 and earlier.
- Storage vMotion from protection storage to primary storage.

All types of recoveries are performed from the **Restore > 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 **Restore > 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 DD system. If a replica backup does not exist on such storage, you must manually replicate this backup to DD 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.


Restoring a virtual machine backup with the storage policy association

vSphere storage-based policies are used to communicate to the storage system details about how the virtual machine and its contents should be stored. At the time of backup, the existing policy assignments for the virtual machine will be stored in the backup copy.

During a restore to the original virtual machine in the PowerProtect Data Manager UI or the **vSphere Client**, you can select the **Restore Storage Policies** option if you want to restore any virtual machine disk-level or non-disk specific storage policy assignments.

This option is only applicable to virtual machine backup copies taken with PowerProtect Data Manager 19.6 and later. If you select this option but the virtual machine backup copy was created with PowerProtect Data Manager version 19.5 and earlier,

or the storage policy has been deleted from the vCenter Server, the virtual machine restore will proceed but any storage policy association will not be restored.

 **NOTE:** Enabling this option requires vCenter version 6.7 and later.

Prerequisites to restore a virtual machine

Review the following requirements before you restore a virtual machine in PowerProtect Data Manager:

- Only the Administrator and the Restore Administrator roles can restore data.
- Ensure that you have added protection storage and the vCenter server, and that the protection of virtual machine copies has completed successfully.

To check, select **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 **Restore > Assets** window.
- If performing a restore to the original virtual machine, a minimum vCenter version 6.7 is required if you want to restore the virtual machine protection policy backup's storage policy assignments.
- 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.
- For restores of virtual machine protection policy backups using the Transparent Snapshot Data Mover (TSDM) protection mechanism, note the following:
 - For a **Restore to Original Folder and Overwrite Original Files**, the virtual machine must be currently protected by a policy that uses TSDM.
 - For a **Create and Restore to New VM**, the destination ESXi host where the new virtual machine will be created must have the vSphere Installation Bundle (VIB) installed and enabled.


Restore to the original virtual machine

A **Restore to Original Folder and Overwrite Original Files** recovers a virtual machine backup to its original location on the vCenter. This operation rolls the virtual machines 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.

Prerequisites


Review [Prerequisites to virtual machine restore](#) before performing the restore.

About this task

 **NOTE:** If the original virtual machine was deleted, a **Restore to Original Folder and Overwrite Original Files** 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.

Steps

1. From the PowerProtect Data Manager UI, select **Restore > Assets**, and then select the **Virtual Machine** tab.
The **Restore** window displays all virtual machines available for restore.
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 asset name of the specific virtual machine or use the **File Search** button to search on specific criteria for files within backed-up virtual machines.
The **Restore** 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 DD 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**.

NOTE: If you specified any disk exclusions in the virtual machine protection policy, a message appears indicating that disks were excluded from this backup. If one of the excluded disks was a boot disk, the restore might not complete successfully.

The **Restore Type** page appears.

7. On the **Restore Type** page:

- a. Select **Restore to Original Folder and Overwrite Original Files**.

NOTE: If the system determines that the original virtual machine datastore(s) may be insufficient to complete the restore a warning is displayed. In this case, create more space in the original datastore(s), and then, select **Proceed Anyways**.

- b. Select the **Restore VM Tags** checkbox to restore vCenter tags and categories associated with this backup copy. Tags are backed up by default as part of the virtual machine protection policy backup.

NOTE: You can only select this option when restoring entire virtual machines. Any existing tags and categories on the assets in the restore location will be replaced with the tags and categories from the assets in the restored copy. If the tags and categories being restored do not exist in the vCenter Server at the time of the restore, or have been deleted, they will be re-created as part of the restore, along with the tag description and the cardinality settings that determine the relationship of tags within a category. If tags and categories on the vCenter have been renamed since the last backup, the renamed tags and categories will not be overwritten upon restore. For example, if a tag's ID is the same but the tag's name has been changed since the backup, a new tag is created based on the tag name in the backup copy being restored.

Upon successful restore, the replaced tags and categories will not be deleted in the **vSphere Client**, and can be viewed in the **Tags & Custom Attributes** window, or the **Tags** pane of the **Summary** window when the virtual machine is selected.

- c. Select **Restore Storage Policies** if you also want to restore any virtual machine disk-level or non-disk specific storage policy assignments.

If you select this option but the backup copy was taken with PowerProtect Data Manager 19.5 and earlier, or the storage policy is not available, the virtual machine restore will proceed but any storage policy association will not be restored.

NOTE: Enabling this option requires vCenter version 6.7 and later.

- d. For low-bandwidth environments, select **Enable DDBoost Compression**.

This option reduces network usage by compressing data on the protection storage system before transfer to the VM Direct Engine, which decompresses the data. Compression reduces restore times but increases CPU usage on both systems.

8. Click **Next**.

The **Networks** page appears if the virtual machine was backed up using PowerProtect Data Manager 19.9 or later. Otherwise, the **Options** page appears.

9. The **Networks** page displays the network adaptors and associated networks the virtual machine had used when it was backed up. Click **Next** after reviewing this information and optionally performing one or both of the following actions.

NOTE: If a network used by an adapter is no longer accessible to the current virtual machine, a warning is displayed, and a different network should be selected for that adapter.

- a. To select a different network, click the associated drop-down control in the **Network** column, and then select an entry from the list.
- b. To change the initial power-on connection status of a network adapter, select or clear the associated check box in the **Connect at Power On** column.

If the current virtual-machine disk configuration is identical to the copy being restored, the **Summary** page appears, but if there is a mismatch, the **Options** page appears. This page displays the current configuration of the virtual machine along with any disks that have been added since the last backup.

10. On the **Options** page, for any hard disks in the current virtual machine configuration that were not part of the backup copy:

- Select **Delete disks that will be detached** to remove these disks upon restore.

- Clear **Delete disks that will be detached** to keep these disks in their original folders on the virtual machine after the restore. 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.

11. 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.

12. On the **Summary** page, click **Restore**.

An informational dialog box appears indicating that the restore has started.

13. 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 **Restore Individual Virtual Disks** recovers individual virtual disks (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.

Prerequisites

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.

Steps

1. From the PowerProtect Data Manager UI, select **Restore > Assets**, and then select the **Virtual Machine** tab.

The **Restore** window displays all virtual machines available for restore.

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 or click the **File Search** button to search on specific criteria.

The **Restore** 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 DD 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 Individual Virtual Disks** to restore specific VMDKs.

7. For low-bandwidth environments, select **Enable DDBoost Compression**.

This option reduces network usage by compressing data on the protection storage system before transfer to the VM Direct Engine, which decompresses the data. Compression reduces restore times but increases CPU usage on both systems.

8. Click **Next**.

The **Select Disks** page displays.

9. 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.

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 to a new virtual machine

A **Create and Restore to New VM** 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.

Prerequisites

Review [Prerequisites to virtual machine restore](#) before you perform this procedure.

Steps

1. From the PowerProtect Data Manager UI, select **Restore > Assets**, and then select the **Virtual Machine** tab.
The **Restore** window displays all virtual machines available for restore.
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 or click the **File Search** button to run file level restore workflows on specific files within VMs.
The **Restore** 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 DD 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** if you want to restore an image-level virtual machine backup.
 **NOTE:** If you specified any disk exclusions in the virtual machine protection policy, a message appears indicating that disks were excluded from this backup. If one of the excluded disks was a boot disk, the restore might not complete successfully.
 - Select **Restore Individual Virtual Disks** if you want to restore only specific VMDKs.
 **NOTE:** Individual disks can only be restored to the original location.
7. Click **Next**.
8. On the **Restore Type** page:
 - a. Select **Create and Restore to New VM**.
 - b. Select the **Restore VM Tags** checkbox to restore vCenter tags and categories associated with this backup copy. Tags are backed up by default as part of the virtual machine protection policy backup.
 **NOTE:** You can only select this option when restoring entire virtual machines. Any existing tags and categories on the assets in the restore location will be replaced with the tags and categories from the assets in the restored copy. If the tags and categories being restored do not exist in the vCenter Server at the time of the restore, or have been deleted, they will be re-created as part of the restore, along with the tag description and the cardinality settings that determine the relationship of tags within a category. If tags and categories on the vCenter have been renamed since the last backup, the renamed tags and categories will not be overwritten upon restore. For example, if a tag's ID is the same but the tag's name has been changed since the backup, a new tag is created based on the tag name in the backup copy being restored.
Upon successful restore, the replaced tags and categories can be viewed in the **vSphere Client Tags & Custom Attributes** window, or the **Tags** pane of the **Summary** window when the virtual machine is selected.
 - c. For low-bandwidth environments, select **Enable DDBoost Compression**.
This option reduces network usage by compressing data on the protection storage system before transfer to the VM Direct Engine, which decompresses the data. Compression reduces restore times but increases CPU usage on both systems.
 - d. Click **Next**.
9. On the **VM Information** page:
 - a. 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.

- b. Select the destination data center.
- c. Click **Next**.

10. On the **Restore Location** page:

- a. 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.
- b. If you select an ESXi host within this page, the next page is unnecessary.
- c. Click **Next**.

11. 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.

12. On the **Datastore** page, select the datastore where you want to restore the virtual machine disks.

NOTE:

The **Total Estimated Space Needed for Recovery** is displayed and updated according to the specified disk provisioning type.

In the datastore list:

- The free space in each datastore is displayed.
- If a datastore is estimated to be smaller than required for recovery, it is displayed in red alongside an error icon.
- Select **Browse...** to display the total capacity, provisioned capacity, and free capacity of all available datastore(s), and select a datastore.

- a. If you are restoring multiple virtual machines, select the **Datastore** and **Provisioning Type** to use for all virtual machines.
- b. If you are restoring one virtual machine:
 - To restore all disks to the same location, keep **Configure Per Disk** disabled, and select the datastore from the datastore list in the **Storage** column.
 - To restore disks to different locations, enable **Configure Per Disk**, and for each disk, select a datastore from the datastore list in the **Storage** column. Select how to provision the disk from the provisioning types in the **Disk Format** column.

NOTE: If you select a datastore whose estimated free space is smaller than required for recovery, a warning is displayed. In this case, you can select **Proceed Anyways** to continue, but it is recommended to create more space in the specified datastore(s) before doing so.

- c. Click **Next**.

13. The **Networks** page appears if the virtual machine was backed up using PowerProtect Data Manager 19.9 or later. It displays the network adaptors and associated networks the virtual machine had used when it was backed up. Click **Next** after reviewing this information and optionally performing one or both of the following actions.

NOTE: If a network used by an adapter is no longer accessible to the new virtual machine, a warning is displayed, and a different network should be selected for that adapter.


- a. To select a different network, click the associated drop-down control in the **Network** column, and then select an entry from the list.
- b. To change the initial power-on connection status of a network adapter, select or clear the associated check box in the **Connect at Power On** column.

14. 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 turned on while temporarily accessing the VMDKs from DD storage. Storage vMotion is initiated to the target datastore. The virtual machine becomes available for use when it is turned 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**.

15. On the **Summary** page, verify that the information you specified in the previous steps is correct, and then click **Restore**.

16. 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, when the instant access session has been created.

Instant access virtual machine restore

An **Instant Access VM** restore enables you to create a new virtual machine directly from the original virtual machine backup on protection storage 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 protection storage to the production datastore. An instant access virtual machine restore also provides the option to move the virtual machine to a production datastore when you want to retain access to the virtual machine for a longer time.

Steps

1. From the PowerProtect Data Manager UI, select **Restore > Assets**, and then select the **Virtual Machine** tab.

The **Restore** window displays all virtual machines available for restore.


2. Select the check box 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, or click the **File Search** button to search on specific criteria.

The **Restore** 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 DD 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** if you want to restore an image-level virtual machine backup.

 **NOTE:** If you specified any disk exclusions in the virtual machine protection policy, a message appears indicating that disks were excluded from this backup. If one of the excluded disks was a boot disk, the restore might not complete successfully.


- Select **Restore Individual Virtual Disks** if you want to restore only specific VMDKs.

 **NOTE:** Individual disks can only be restored to the original location.

7. On the **Restore Type** page:

a. Select **Instant Access VM**.

b. Select the **Restore VM Tags** checkbox to restore vCenter tags and categories associated with this backup copy.

 **NOTE:** You can only select this option when restoring entire virtual machines. Any existing tags and categories on the assets in the restore location will be replaced with the tags and categories from the restored copy. If the tags and categories being restored do not exist in vCenter at the time of the restore, or have been deleted, they will be re-created as part of the restore, along with the tag description and the cardinality settings that determine the relationship of tags within a category. If tags and categories on the vCenter have been renamed since the last backup, the renamed tags and categories will not be overwritten upon restore. For example, if a tag's ID is the same but the tag's name has been changed since the backup, a new tag is created based on the tag name in the backup copy being restored.

Upon successful restore, the replaced tags and categories can be viewed in the **vSphere Client Tags & Custom Attributes** window, or the **Tags** pane of the **Summary** window when the virtual machine is selected.



c. Click **Next**.

8. 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**.
9. 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 ESXi host within this page, the next page is unnecessary. Click **Next**.
10. 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.
11. The **Networks** page appears if the virtual machine was backed up using PowerProtect Data Manager 19.9 or later. It displays the network adaptors and associated networks the virtual machine had used when it was backed up. Click **Next** after reviewing this information and optionally performing one or both of the following actions.
-  **NOTE:** If a network used by an adapter is no longer accessible to the new virtual machine, a warning is displayed, and a different network should be selected for that adapter.
- a. To select a different network, click the associated drop-down control in the **Network** column, and then select an entry from the list.
 - b. To change the initial power-on connection status of a network adapter, select or clear the associated check box in the **Connect at Power On** column.
12. On the **Options** page:
- a. Specify a name for the Instant Access virtual machine.
 - b. Optionally, 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 for instant access virtual machine restores.
 - c. Click **Next**.
13. 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.
14. 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, when the instant access session has been created.


Results

To monitor and manage the instant access virtual machine recovery, select **Restore > Running Sessions**, and then click the **Instant Access** tab. From this window, you can also extend the instant access virtual machine session beyond the default period of 7 days.

 **NOTE:** On a single-node protection storage system such as a DD system, instant access/restore functionality has been enhanced to return a failure message when overwhelmed with traffic. For example, if on the target node or the ESXi host there are Live VM and/or Instant Restore sessions that are in conflict, instant access/restore jobs will fail with a message indicating a resource contention issue. If this occurs, you need to clear the conflicts and then restart the session in order for the job to execute.

Manage and monitor Instant Access sessions

In the PowerProtect Data Manager UI, the **Instant Access** tab of the **Restore > Running Sessions** window enables you to monitor vMotion events, and to manage the status of a virtual machine restore to new or instant access virtual machine restore. For example, you can extend the availability period or delete an instant access virtual machine.

 **NOTE:** The Instant Access Sessions that are 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 **Restore > Running Sessions > Instant Access** to access information about the sessions. This window enables you to monitor and manage all exported copies that you have created from protection storage. 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 the vCenter server, and PowerProtect Data Manager removes 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.

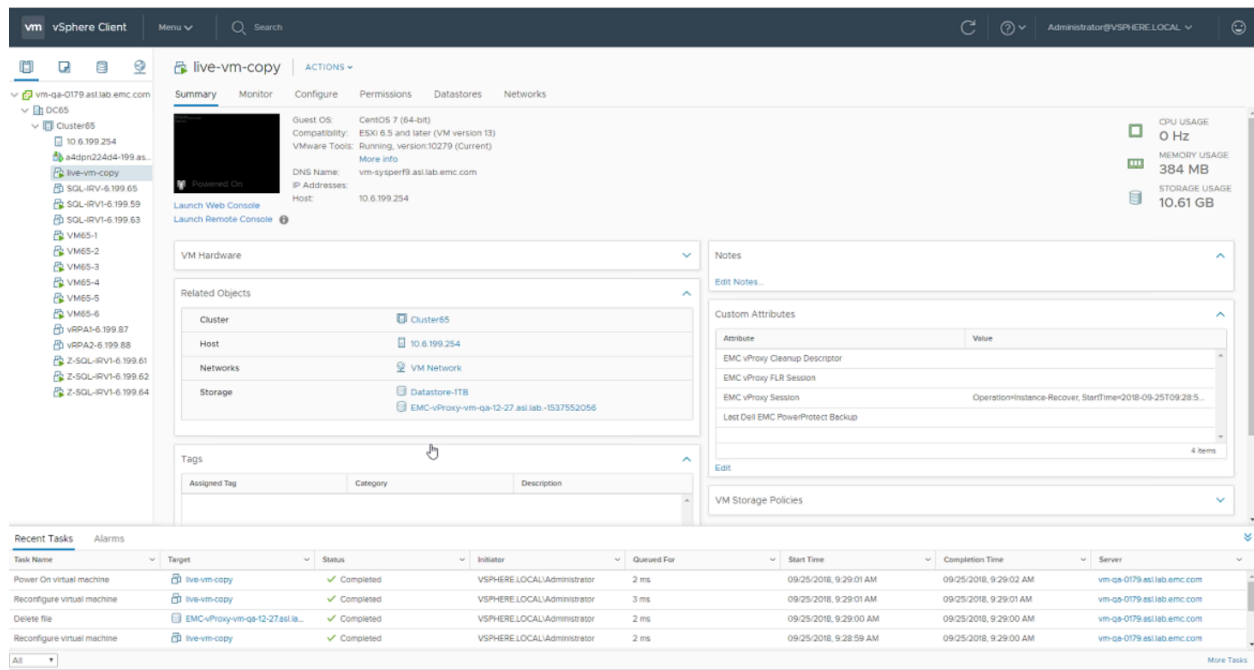



Figure 3. Instant access virtual machine restore in the vSphere Client

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 select the session and move the virtual machine to a production datastore.

Steps

1. From the PowerProtect Data Manager UI, select **Restore > Running Sessions**, and then click the **Instant Access** 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** 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** 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** window.

File level restore to original virtual machine

A file level restore to original virtual machine enables you to recover individual files from backups of virtual machines or VMDKs performed in PowerProtect Data Manager to the same or a new location on the original vCenter Server. Only the Administrator and the Restore Administrator roles can restore data.


Prerequisites

- Review the section [Supported platform versions for file-level restore](#) for supported platform and operating system versions.
- Review the section [File-level restore and SQL restore limitations](#) on page 247.

 **NOTE:** For file-level restores, you can only restore files:

- From a Windows backup to a Windows machine, or from a Linux backup to a Linux machine.
- To virtual machines within the same vCenter.

Steps

1. From the PowerProtect Data Manager UI, select **Restore > Assets**, and then select the **Virtual Machine** tab.
The **Restore** window displays all the virtual machines available for restore.
 2. Select the checkbox next to the virtual machine that you want to recover from, and then click **View Copies**.
You can also use the filter in the **Name** column to search for a specific virtual machine name, or click the **File Search** button to search on specific criteria.
The **Restore > 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 location in the left pane, for example, a DD system, the copies on that system display in the right pane.
 3. If the backup is on a DD 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 **Restore Type** page, select **Restore to Original Virtual Machine**, and then click **Next**.
 6. On the **Mount Copy** page:
 - a. To initiate the disk mount, type the guest operating system user credentials:
 - If there are administrator-level credentials associated with the virtual assets or protection policy being restored, specify end-user credentials.
 - If there are no administrator-level credentials associated with the virtual assets or protection policy being restored, specify administrator credentials. These credentials will be handled as end-user credentials.
 - b. (Optional) Leave **Keep FLR Agent Installed** selected when 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 indicates when the mount completes.
 **NOTE:** You cannot browse the contents of the virtual machine backup until the mounting of the destination virtual machine completes successfully.
- When validated, the **FLR Agent** is installed automatically on the restore destination, if it is not already installed. The **FLR Agent** facilitates the mounting and unmounting of disks and the browsing of files in the destination virtual machine and the backup copy. In order to complete the automatic **FLR Agent** installation, on Windows virtual machines the user must be an administrator account, and on Linux virtual machines the user must be the root user account, or a user in the operating system's local sudousers list. The section [FLR Agent for virtual machine file level restore](#) on page 248 provides more information.
- d. Upon successful mount, 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 that you want to restore to the destination virtual machine.
 - b. Click **Next**.

NOTE: When you browse for objects to recover on this page, each directory or hard drive appears twice. As a result, when you select an object from one location, the object is selected in the duplicate location as well.

8. On the **Options** page, select from one of the following options, and then click **Next**.
 - Restore to Original Folder and Overwrite Original Files—Select this option to restore all selected files to their original location on the original virtual machine.
 - Restore to an Alternate Folder—Select this option if you want to restore to a new folder in a new location on the original virtual machine.
9. On the **Summary** page:
 - a. Review the information to ensure that the restore details are correct. You can click **Edit** next to any row to change the information.
 - b. Click **Restore**.
10. Go to the **Jobs** window to monitor the restore.

A restore job appears with a progress bar and start time.

File level restore to alternate virtual machine

A file level restore to alternate virtual machine enables you to recover individual files from backups of virtual machines or VMDKs performed in PowerProtect Data Manager to a new location on a new virtual machine. This restore can be performed to a primary or secondary vCenter Server. Only the Administrator and the Restore Administrator roles can restore data.

Prerequisites

- Review the section [Supported platform versions for file-level restore](#) for supported platform and operating system versions.
- Review the section [File-level restore and SQL restore limitations](#) on page 247.

NOTE: For file-level restores, you can only restore files:

- From a Windows backup to a Windows machine, or from a Linux backup to a Linux machine.
- To virtual machines within the same vCenter.

Steps

1. From the PowerProtect Data Manager UI, select **Restore > Assets**, and then select the **Virtual Machine** tab.

The **Restore** window displays all the virtual machines available for restore.
2. Select the checkbox next to the virtual machine that you want to recover from, and then click **View Copies**.

You can also use the filter in the **Name** column to search for a specific virtual machine name, or click the **File Search** button to search on specific criteria.

The **Restore > 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 location in the left pane, for example, a DD system, the copies on that system display in the right pane.
3. If the backup is on a DD 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 **Restore Type** page, select **Restore to Alternate Virtual Machine**, and then click **Next**.
6. On the **Select Target VM** page, choose from one of the following options:
 - Search for a target virtual machine by typing the name.
 - Browse from the available vCenter Servers to locate the destination virtual machine.
7. On the **Mount Copy** page:
 - a. To initiate the disk mount, type the guest operating system user credentials:
 - If there are administrator-level credentials associated with the virtual assets or protection policy being restored, specify end-user credentials.
 - If there are no administrator-level credentials associated with the virtual assets or protection policy being restored, specify administrator credentials. These credentials will be handled as end-user credentials.
 - b. (Optional) Leave **Keep FLR Agent Installed** selected when 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 indicates when the mount completes.

NOTE: You cannot browse the contents of the virtual machine backup until the mounting of the destination virtual machine completes successfully.

When validated, the **FLR Agent** is installed automatically on the restore destination, if it is not already installed. The **FLR Agent** facilitates the mounting and unmounting of disks and the browsing of files in the destination virtual machine and the backup copy. In order to complete the automatic **FLR Agent** installation, on Windows virtual machines the user must be an administrator account, and on Linux virtual machines the user must be the root user account, or a user in the operating system's local sudousers list. The section [FLR Agent for virtual machine file level restore](#) on page 248 provides more information.

- d. Upon successful mount, click **Next**.

8. On the **Select Files to Recover** page:

- a. Expand individual folders to browse the original virtual machine backup, and select the objects that you want to restore to the destination virtual machine.
- b. Click **Next**.

NOTE: When you browse for objects to recover on this page, each directory or hard drive appears twice. As a result, when you select an object from one location, the object is selected in the duplicate location as well.

9. On the **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**.

10. On the **Summary** page:

- a. Review the information to ensure that the restore details are correct. You can click **Edit** next to any row to change the information. If you are not restoring to the original virtual machine, an additional field appears for the **Target VM**.
- b. Click **Restore**.

11. 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.

Prerequisites

Direct Restore to ESXi restore requires either the embedded VM Direct engine with PowerProtect Data Manager, or an external VM Direct appliance that is added and registered to PowerProtect Data Manager.

Additionally, ensure that you disconnect the ESXi host from the vCenter server.

Steps

1. From the PowerProtect Data Manager UI, select **Restore > Assets**, and then select the **Virtual Machine** tab.
The **Restore** window displays all of the virtual machines available for restore.

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 or click the **File Search** button to search on specific criteria.

The **Restore > 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 DD system, the copies on that system display in the right pane.

3. If the backup is on a DD 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. For low-bandwidth environments, select **Enable DDBoost Compression**.
This option reduces network usage by compressing data on the protection storage system before transfer to the VM Direct Engine, which decompresses the data. Compression reduces restore times but increases CPU usage on both systems.
 - c. Click **Next**.
6. On the **ESX Host Credentials** page:
 - a. In the **ESX Host** field, type the IP of the ESXi server where you want to restore the virtual machine backup.
 - b. Specify the root **Username** and **Password** for the ESXi 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, or perform a centralized restore within the PowerProtect Data Manager UI.

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.

Restore the PowerProtect Data Manager server

You can restore PowerProtect Data Manager server persisted data as a new instance using any of the backups. Only the Administrator role can carry out the restore.

Prerequisites

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.

Steps

1. Deploy the PowerProtect Data Manager OVA and power it on.
2. Select **Restore Backup**.

To delay jobs defined by your protection policies until otherwise specified, select **After restore, keep the product in recovery mode so that scheduled workflows are not triggered**. When selected, after restore the system enters recovery maintenance mode. During recovery maintenance mode:

- All jobs defined by your protection policies that modify the backup storage (for example, backup creation, backup deletion, and PowerProtect Data Manager Server DR jobs) are not triggered.
- All operations that write to the backup storage are disabled.
- A system alert is displayed in PowerProtect Data Manager.



To enable automatically scheduled operations and user operations that write to the backup storage, click **Return to full Operational mode** in the alert.

3. Specify the following storage information:
 - a. DD system IP where the recovery backups are stored.
 - b. DD 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 then click **OK**.
5. Select the backup file that you would like to use for recovery, and then click **Recover**.
6. Specify the lockbox passphrase associated with the backup, and start the recovery.
This step initiates 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.

Results

The PowerProtect Data Manager server is recovered.

Next steps

After a successful recovery:

- The time zone of the PowerProtect Data Manager instance is set to the same as that of the backup.
- All preloaded accounts are reset to default passwords, as described in the *PowerProtect Data Manager Security Configuration Guide*. The preloaded UI administrator account is an exception and retains its password. Change the passwords for all preloaded accounts as soon as possible.

Restore Cloud Tier backups to protection storage


Once a Cloud Tier backup is recalled, restore operations of these backups are identical to normal restore operations.

The PowerProtect Data Manager software recalls a copy of the backup from the Cloud unit to the local (active) tier of protection storage, which then allows you to perform a restore of the backup from the active tier to the client. The status appears as **Cloud**, and changes to **Local Recalled** after cloud recall completes. After the restore, the backup copy is removed from Cloud Tier, and is stored on the active tier of protection storage for a minimum of 14 days, after which the backup may be returned to the cloud depending on your protection policy.

Recall and restore from Cloud Tier


Perform the following steps to recall a backup on Cloud Tier to the active tier on protection storage and restore this backup.

Prerequisites

 **NOTE:** When a backup is recalled from Cloud Tier to the active tier, the copy is removed from Cloud Tier.

Steps

1. From the PowerProtect Data Manager UI, select **Infrastructure > Assets**.
2. On the **Assets** window, select the tab that contains the asset you want to recall from Cloud Tier, and then click **View Copies**.
3. Click **DD**, and then select from one of the available copies that appear in the table.
4. Click **Recall**.
The **Recall from Cloud** dialog box appears.
5. In the **Retain until** box, specify how long you want to keep the copy on the active tier, and then click **OK**.
6. Go to the **Jobs** window to monitor the recall operation.
When the copy has been moved successfully, the **Location** changes from Cloud to Local.

7. Select **Restore > Assets**, and then select the tab that contains the recalled asset.
8. Select the recalled asset, and then click **Restore**.
 -  **NOTE:** If you are unsure whether the asset has been recalled, click **View Copies** and select **DD** to view the available backup copies. If the asset backup is a recalled copy, the Status column indicates **Local Recalled**.
9. Select the recalled copy to re-tier the copy to the active tier.

Preparing for and Recovering From a Disaster

Topics:

- [Managing system backups for server disaster recovery](#)
- [Prepare the DD system recovery target \(NFS\)](#)
- [Configure PowerProtect Data Manager server DR backups](#)
- [Record settings for server DR](#)
- [Manage PowerProtect Data Manager server DR backups](#)
- [Restore PowerProtect Data Manager from server DR backups](#)
- [Troubleshooting NFS backup configuration issues](#)
- [Troubleshoot recovery of PowerProtect Data Manager](#)
- [Quick recovery](#)
- [Recover a failed PowerProtect Data Manager backup](#)

Managing system backups for server disaster recovery

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 disaster recovery (DR) 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 protection storage, full user functionality is restored.

The system protection service enables you to manage the frequency and retention of an automated server DR backup. You can also perform manual backups. However, the system protection service does not manage the retention of manual backups and you must delete any outdated manual backups yourself. [Manage PowerProtect Data Manager server DR backups](#) on page 129 provides instructions.

File Search indexes are backed up for DR recovery along with other component DR backups.

You can back up to only one protection storage system at a time. When you specify a new protection storage system for backup, you overwrite the existing protection storage system selection. If you have more than one protection storage system, you can change which protection storage system holds the server DR backup.

Server DR protection storage types

PowerProtect Data Manager supports two types of protection storage for server DR: NFS and DD Boost.

Updating the PowerProtect Data Manager server does not automatically change the storage type. Instead, select the appropriate storage type and manually configure server DR backups. Do not alternate between storage types.

Switching from NFS to DD Boost creates new server DR backups, rather than migrating existing backups. The previous NFS backups are no longer visible in the list of DR backups. However, you can still recover from older NFS server DR backups even after switching to DD Boost, should you experience a disaster before the initial DD Boost system backup completes.

NFS

NFS is the legacy storage type for PowerProtect Data Manager server DR. To store backups over NFS, you must configure and assign a private storage unit for the PowerProtect Data Manager system. Then, prepare the DD recovery target by creating an

NFS export. With the DD system address and the NFS export path, you can configure PowerProtect Data Manager to perform server DR backups.

Starting with PowerProtect Data Manager 19.9, NFS storage is deprecated.

DD Boost

DD Boost is the recommended storage type for PowerProtect Data Manager server DR. DD Boost provides security and efficiency advantages over NFS, including password-protected authentication. When you use DD Boost, PowerProtect Data Manager creates and manages a storage unit on the DD system and a corresponding user account.

The storage unit and user account name are based on the PowerProtect Data Manager hostname. For example, `SysDR_<hostname>`. The DD Boost user password is based on the PowerProtect Data Manager predefined administrator account password. Changes to the predefined administrator account password prompt corresponding updates to the DD Boost user password. Recovery from server DR backups requires the predefined administrator account password. If you do not know this password, contact Customer Support.

If you plan to use DD Boost, add the DD system as protection storage before you configure server DR. [Protection storage](#) on page 38 provides instructions.

Overview of PowerProtect Data Manager Cloud Disaster Recovery

The Cloud Disaster Recovery (DR) feature enables you to utilize a cloud DR site by deploying the Cloud DR Server in the public cloud. You can use the PowerProtect Data Manager UI for the purpose of running VM protection and DR workflows in the cloud.

Examples of Cloud DR workflows include the following:

- Cloud DR site copy management—Set the Cloud DR site by creating a VM protection policy in the PowerProtect Data Manager UI.
- VM copy failover validation—Before a disaster occurs, you can validate the failover of a VM copy to the cloud within PowerProtect Data Manager by running a DR test and then monitoring the test progress.
- Fail over a production VM—You can fail over a production virtual machine within PowerProtect Data Manager by running a DR failover operation and then verifying that the restored VM appears within Amazon Web Services (AWS) or Microsoft Azure cloud.


The *PowerProtect Data Manager Cloud Disaster Recovery Administration and User Guide* provides more information about Cloud DR workflows within PowerProtect Data Manager.

Prepare the DD system recovery target (NFS)

If you plan to use NFS for system backup storage, configure the NFS export on the DD target system and select the required permissions. Configuring PowerProtect Data Manager for backup and recovery requires this NFS export path.

Steps

1. Use a web browser to log in to DD System Manager as the system administrator user.
2. On 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 DD MTree.
 - **Directory Path**—the full directory path for DD MTree that you created. Ensure that you use the same name for the directory.

 **NOTE:** For an external DD system, specify a path similar to the following, `/data/col1/<path>`, where `<path>` is the MTree that stores the system 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 DD 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 hostname of the PowerProtect Data Manager.



NOTE: To configure DR protection for an existing Search cluster, add the IP address or hostname of the Search cluster to the NFS client list.

- 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 PowerProtect Data Manager to change the directory structure on the NFS share.

Configure PowerProtect Data Manager server DR backups


Configure DR protection for the PowerProtect Data Manager system and the system metadata.

Prerequisites

If you plan to use NFS for protection storage, prepare the target DD system as described in [Prepare the DD system recovery target \(NFS\)](#) on page 127.

If you plan to use DD Boost for protection storage, add the DD system as protection storage. [Protection storage](#) on page 38 provides instructions.

Steps

1. Log in to the PowerProtect Data Manager user interface as a user with the Administrator role.
2. Click , select **Disaster Recovery**, and then click **Configuration**.
3. Select **Enable backup**.
4. For NFS, configure the backup with the following attributes:
 - a. For **Protocol**, select **NFS**.
 - b. In the **PowerProtect DD System** field, type the IP address or hostname of the DD system for the backup.
 - c. In the **NFS Export Path** field, type the NFS path where server DR backups are stored on the target DD system.
5. For DD Boost, configure the backup with the following attributes:
 - a. For **Protocol**, select **DDBoost**.
 - b. From the **PowerProtect DD System** drop-down list, select an existing protection storage system.
For initial DR configuration, the **Storage Unit** field is empty. If DR was already configured, the **Storage Unit** field displays the name of the storage unit that holds server DR backups.
6. Configure the backup frequency and duration:
 - a. Type an interval between server DR backups, in hours.
This setting controls backup frequency, and the allowed values are 1 to 24 hours.
 - b. Type the number of days for which PowerProtect Data Manager should retain server DR backups.
The allowed values are 2 to 30 days.
7. Click **Save**.

Results

For DD Boost, PowerProtect Data Manager creates system jobs to prepare the new storage unit and to configure the server DR protection policy.

For both storage types, PowerProtect Data Manager creates a system job for the first server DR backup.


Next steps

Verify that the system jobs succeed.

Record settings for server DR

Plan for DR by recording vital information. In the event of a major outage, you will need certain information to recover your systems. Record the following information on a local drive outside PowerProtect Data Manager:

Steps

1. Log in to the PowerProtect Data Manager user interface as a user with the Administrator role.
2. Record the PowerProtect Data Manager build number.
Customer Support can provide this information, which is not mandatory.
3. Record the PowerProtect Data Manager hostname.
4. Record the port groups:
 - a. Log in to the vSphere client.
 - b. Right-click the appliance name and select **Edit Settings**.
 - c. Record the port group settings that are assigned to PowerProtect Data Manager.
5. Click , select **Disaster Recovery**, and then click **Configuration**.
6. Record whether server DR storage uses NFS or DD Boost.
7. If you use NFS for server DR storage, record the protection storage system IP address or hostname, and the NFS export path.
8. If you use DD Boost for server DR storage, record which protection storage system stores the server DR backups.
Record the protection storage system IP address and hostname or FQDN.
9. Use the REST API to record additional configuration information:
Run the GET /Configurations API (api/v2/configurations) from PowerProtect Data Manager and save the details for network information.

- a. Obtain a PowerProtect Data Manager authentication token:

```
curl --request POST
'https://<ppdm_ip>:8443/api/v2/login' --header
'Content-Type: application/json' --data
'{"username":<user>,"password":<password>}' -k
```

- b. Use the authentication token to get the configuration from PowerProtect Data Manager:

```
curl --request GET
'https://<ppdm_ip>:8443/api/v2/configurations' --header
'Content-Type: application/json' --header
'Authorization: Bearer <token>' -k
```

Manage PowerProtect Data Manager server DR backups

View PowerProtect Data Manager server DR backups and perform manual backups. You can view the last 5 server DR backups.


About this task

For DR backups, PowerProtect Data Manager supports a default retention period of 7 days plus the last 3 hourly backup copies for the current day. You can change the frequency and retention of DR backups from the **Disaster Recovery > Configuration** tab.

The system protection service automatically deletes scheduled backups according to the configured retention policy. You cannot manually delete scheduled backups. However, you can delete manual backups.

Steps

1. Log in to the PowerProtect Data Manager user interface as a user with the Administrator role.


2. Click , select **Disaster Recovery**, and then click **Manage Backups**.
3. To perform a manual 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 by 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 Backup**.

The backup appears as an entry in the table. To view details for the backup, click the arrow icon.

If the Search Engine is deployed, PowerProtect Data Manager also backs up the Search Engine. The backup details provide the status of the Search Engine backup.

To monitor the status of the backup, select **Jobs > Protection** and look for a job with the name **Protect the server datastore**.
4. To delete a backup:
 - a. Select a backup from the list.
 - b. Click  for that row.

The system displays a warning to confirm you want to delete the backup. Click **Yes** to proceed.
5. Click **Cancel**.


Restore PowerProtect Data Manager from server DR backups

You can restore PowerProtect Data Manager from a server DR backup on a protection storage system.

Prerequisites


- Ensure that all the information listed in [Record settings for server DR](#) on page 129 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 DD system recovery target \(NFS\)](#) on page 127.

To restore from DD Boost, ensure that you have the current password for the PowerProtect Data Manager UI predefined administrator account. If you do not know this password, contact Customer Support.

 **NOTE:** If the Search Engine nodes from the previous PowerProtect Data Manager installation are still hosted on the vCenter, delete the Search Engine nodes from the vCenter before you restore the PowerProtect Data Manager system. The disaster recovery process redeploys the Search Engine nodes as part of the restore operation.

About this task

When a 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 DD system.

 **NOTE:** If the recovery system is on a different FQDN, see [Troubleshoot recovery of PowerProtect Data Manager](#) on page 133.

If a Search Engine is present in the recovery backup when you restore the PowerProtect Data Manager system, the Search Engine is automatically restored.

Steps

1. Use the OVA file to deploy a new PowerProtect Data Manager system.
2. On the **Install** window under **Welcome**, select **Restore Backup**.
3. (Optional) To keep the PowerProtect Data Manager server in recovery mode after the restore completes, select the checkbox.

When this option is enabled, PowerProtect Data Manager enters into recovery mode and stops scheduled workflows from running.

4. To restore from NFS:
 - a. For **Protocol**, select **NFS**.
 - b. Under **Select File**, enter the DD System and NFS Export Path where the backup is located, and then click **Connect**.
A list of the available recovery backups appears.
5. To restore from DD Boost:
 - a. For **Protocol**, select **DDBoost**.
 - b. Type the hostname or IP address for the protection storage system that stores server DR backups.
 - c. If the hostname is not already populated, type the hostname for the PowerProtect Data Manager system.
 - d. Type the password for the predefined administrator account.
 - e. Click **Connect**.
A list of the available recovery backups appears.
6. Select the backup from which to recover the system, and then click **Recover**.
The recovery starts. Recovery can take a few minutes.

Results

When recovery is complete, the PowerProtect Data Manager login page appears.

When you log in to PowerProtect Data Manager, If the option to keep the PowerProtect Data Manager server in recovery mode was selected, a red banner appears at the top of the PowerProtect Data Manager UI. The banner indicates that the PowerProtect Data Manager system is operational but scheduled workflows are disabled. If you want to return PowerProtect Data Manager to full operational mode and enable scheduled workflows, click **Return to full operational mode**.

All preloaded accounts are reset to default passwords, as described in the *PowerProtect Data Manager Security Configuration Guide*. The preloaded UI administrator account is an exception and retains its password. Change the passwords for all preloaded accounts as soon as possible.

Recovering the Search Engine from a DR backup

PowerProtect Data Manager automatically restores the Search cluster after disaster recovery of the PowerProtect Data Manager system is complete. If the PowerProtect Data Manager system could not restore the Search cluster automatically, use the steps in this procedure to restore only the Search cluster through the REST API. Recovery of a Search cluster must be performed on an operational PowerProtect Data Manager system. Only the Administrator role can restore the Search cluster.

Prerequisites

Obtain the name of the Search cluster backup from **System Settings > Disaster Recovery > Manage Backups**.

Steps

1. Log in to the PowerProtect Data Manager user interface as a user with the Administrator role.
Use the same credentials that you used before PowerProtect Data Manager was restored.
2. Locate the backup manifest file:
 - a. Connect to the PowerProtect Data Manager console as an admin user.
 - b. Browse the directory path `/data01/server_backups/<PPDM Hostname>_<NodeID>`.
 - c. Run `grep -Rnwa -e '<Name>' --include=*.manifest`
3. Open the backup manifest file.
4. Locate the `Components` section, which contains `Search Cluster`.
The values for the following fields that are listed in the `Search Cluster` section are needed for the POST call in the next step.
 - `Name=id`
 - `BackupPath`, which contains `<NFSSHost>:/data/coll1/<NFSExportFolder>/<NFSDirPath>/SearchCluster`

For example:

```
"Components": [  
  { "name": "SearchCluster",
```

```
{
  "id": "c25290d9-a88c-4a15-9e7c-656f186209ae",
  "version": "v2",
  "backupPath": "10.25.12.74:/data/coll/serverdr_backup/vm-qa-0091_6ce36793-3379-45d2-84bd-d8bde69e52d4/SearchCluster",
  "backupStatus": "SUCCESSFUL",
  "backupsEnabled": true
}
```

where:

- o NFSHost = "10.25.12.74"
- o NFSExport = "/data/coll/serverdr_backup"
- o NFSDirPath = "vm-qa-0091_6ce36793-3379-45d2-84bd-d8bde69e52d4/SearchCluster"
- o Name = "c25290d9-a88c-4a15-9e7c-656f186209ae"

5. Use the REST API to run the following POST call:

```
https://<PPDM IP>:8443/api/v2/search-clusters/component-backups/
<Name>/restore

{
  "ddDirectoryPath" : "<NFSDirPath>",
  "ddHost" : "<NFSHost>",
  "ddNfsExportName" : "<NFSExport>"
}
```

6. To monitor the status of the restore process, in the PowerProtect Data Manager UI, select **Jobs > System Jobs** and look for a job with the description, **Restoring backup Search Node**.

Troubleshooting NFS backup configuration issues

The following sections provide a list of error messages that might appear when you configure a server DR backup configuration that uses NFS.

DD 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 DD system for the full path to the server DR 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.

DD storage unit mount command failed with error: 'Cannot resolve *FQDN*: The name or service not known'

This error message appears when PowerProtect Data Manager cannot contact the DD system by using the specified FQDN. To resolve this issue, ensure that you can resolve the FQDN and IP address of the DD system.

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.

Steps

1. On the DD 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.

Quick recovery

After a disaster, the quick recovery feature allows you to restore assets and data that you replicated to a destination system at a remote site.

Quick recovery sends metadata from the source system to the destination system, following the flow of backup copies. This metadata makes the replication destination aware of the copies and enables the recovery view. You can recover your workloads at the remote site before you have the opportunity to restore the source PowerProtect Data Manager system.

For example, the following figures show two sites that are named A and B, with independent PowerProtect Data Manager and DD systems for protection storage. Each site contains unique assets. Figure [Separate datacenters, before disaster](#) on page 134 shows the initial configuration with both sites replicating copies to each other. Figure [Separate datacenters, after disaster](#) on page 135 shows the aftermath, with site A down. The site A assets have been restored with quick recovery into the site B environment from the replicated copies.

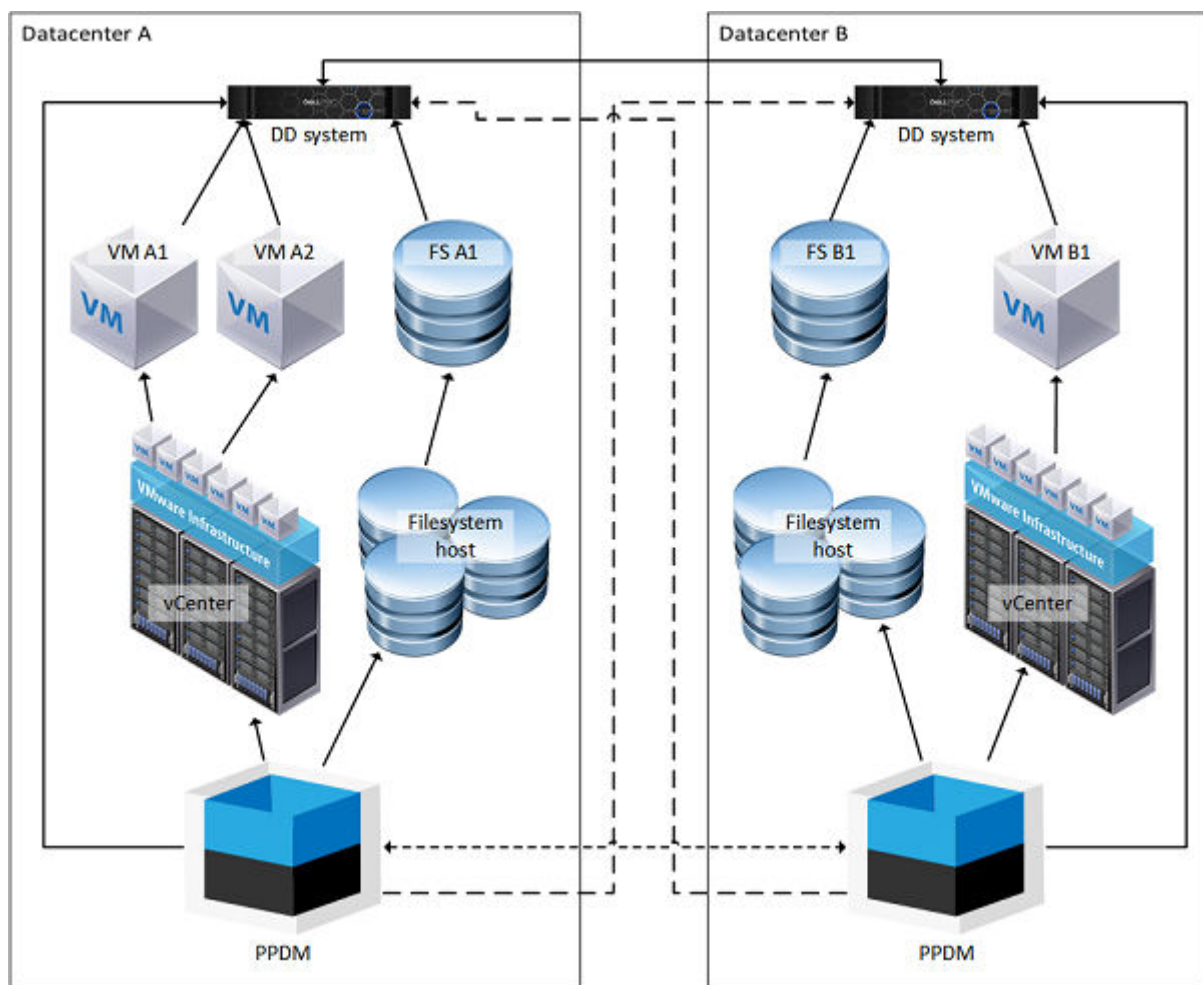


Figure 4. Separate datacenters, before disaster

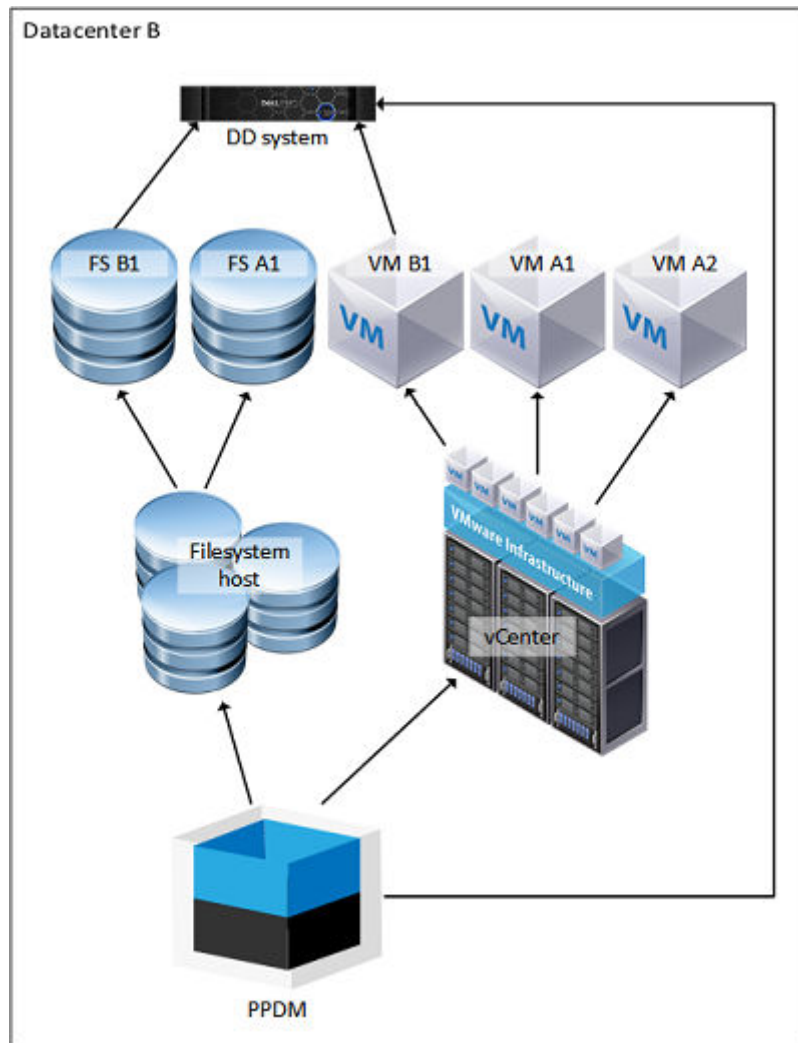


Figure 5. Separate datacenters, after disaster

PowerProtect Data Manager supports quick recovery for alternate topologies. You can configure quick recovery for one-to-many and many-to-one replication. For example, the following figure shows a source PowerProtect Data Manager replicating to a standby DD system with its own PowerProtect Data Manager, all in the same data center. If the source system fails, the quick recovery feature ensures that you can still restore from those replicated copies before you restore the source.

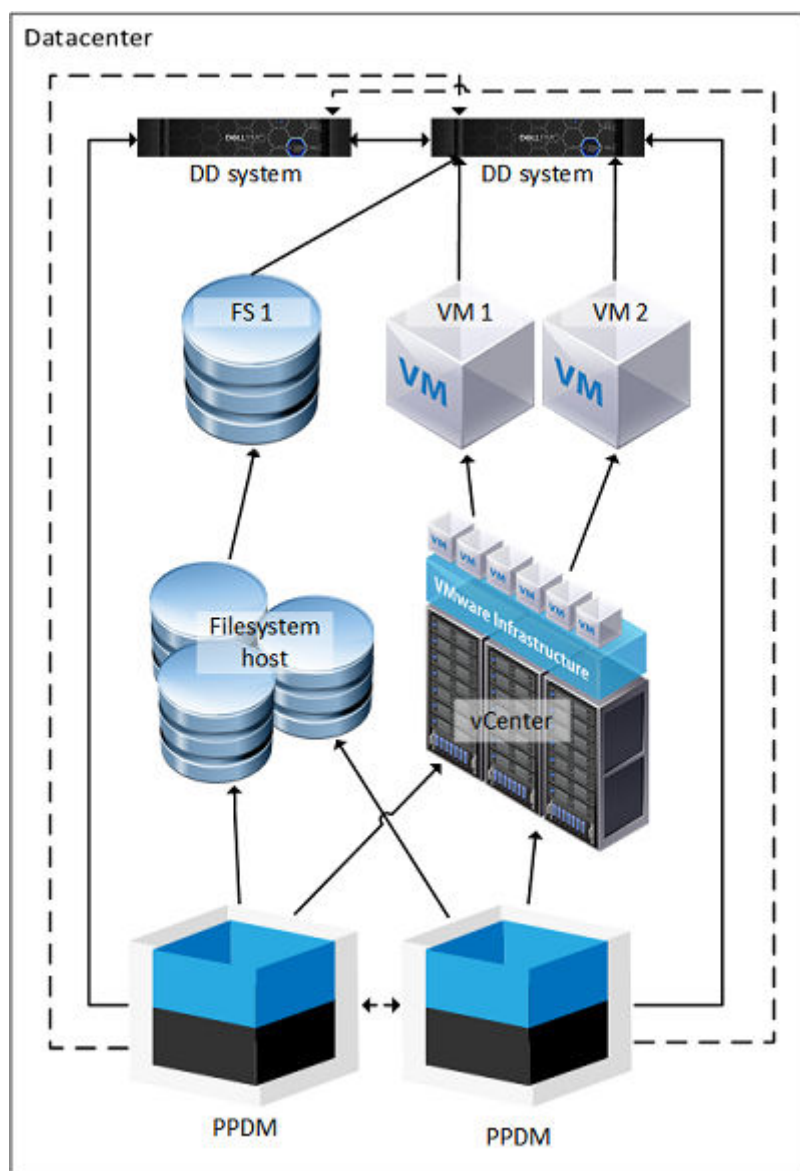


Figure 6. Standby DD system

The following topics explain the prerequisites, how to configure PowerProtect Data Manager to support quick recovery, and how to use the recovery view to restore assets.

Quick recovery prerequisites

Before you configure quick recovery, complete the following items:



- Attach at least two protection storage system systems to the source system: one for local protection storage and one for replication.
- Register asset sources with the source system and configure protection policies to protect those assets.
- Configure protection policies to replicate backup copies to the protection storage system at the remote site.
- Back up the protected assets and confirm that backup data successfully replicates to the destination protection storage system.

Before you use the quick recovery remote view, add the destination system to the list of remote systems on the source.

Add a remote system for quick recovery

Configure PowerProtect Data Manager to send metadata to another system to which you have replicated backups. Only the Administrator role can add remote systems.

Steps

1. Click , select **Disaster Recovery**, and then click **Remote Systems**.
The **Remote Systems** tab opens and displays a table of configured remote PowerProtect Data Manager systems.
2. Click **Add**.
The **Add Remote PowerProtect System** window opens.
3. Complete the **Name** and **FQDN/IP** fields.
The **Name** field is a descriptive name to identify the remote system.
4. In the **Port** field, type the port number for the REST API on the remote system.
The default port number for the REST API is 8443.
5. From the **Credentials** field, select an existing set of credentials from the list.
Alternatively, you can click **Add Credentials** from this list to add new credentials. Provide a descriptive name for the credentials, a username, and a password. Then, click **Save** to store the credentials.
6. Click **Verify**.
PowerProtect Data Manager contacts the remote system and obtains a security certificate for identity verification.
The **Verify Certificate** window opens to present the certificate details.
7. Review the certificate details and confirm each field against the expected value for the remote system. Then, click **Accept** to store the certificate.
The **Certificate** field changes to `VERIFIED` and lists the server's identify.
8. Click **Save**.
PowerProtect Data Manager returns to the **Remote Systems** tab of the **Disaster Recovery** window. The configuration change may take a moment to complete.
9. Click **Cancel**.
The **Disaster Recovery** window closes.
10. Click , select **Disaster Recovery**, and then click **Remote Systems**.
The **Remote Systems** tab opens.
11. Verify that the table of remote systems contains the new PowerProtect Data Manager system.
12. Click **Cancel**.
The **Disaster Recovery** window closes.

Next steps

On the remote system, enable the same asset sources that are enabled on this system. [Enable an asset source](#) on page 60 provides more information. Enabling an asset source on the remote system makes replicated backups of that type visible and accessible.

On the remote system, open the recovery view and verify that backups are visible and accessible. Dell Technologies recommends that you perform a test restore.

Metadata syncs between source and destination systems every six hours. If backups are not visible, allow sufficient time for the first sync before troubleshooting.

Edit a remote system

You can change the descriptive name of the remote system, as well as the REST API port number and credentials. Only the Administrator role can edit remote systems.

Steps

1. Click , select **Disaster Recovery**, and then click **Remote Systems**.

The **Remote Systems** tab opens and displays a table of configured remote PowerProtect Data Manager systems.

2. Locate the row that corresponds to the appropriate remote system, and then select the checkbox for that row. The PowerProtect Data Manager enables the **Edit** button.

3. Click **Edit**.
The **Edit Remote PowerProtect System** window opens.

4. Modify the appropriate parameters, and then click **Save**.


If you change the port number, you may need to re-verify the remote system security certificate.

PowerProtect Data Manager returns to the **Remote Systems** tab of the **Disaster Recovery** window. The configuration change may take a moment to complete.

5. Click **Cancel**.
The **Disaster Recovery** window closes.

Quick recovery remote view

Use the remote view to work with replicated copies on the destination system after the source is no longer available. For example, to restore critical assets before you are able to restore the source system.


On the destination system, log in as a user with the Administrator role. The remote server contains an additional **Remote Systems**  icon in the banner.

When you click **Remote Systems**, PowerProtect Data Manager presents a drop-down that contains the names of the local system and any connected systems. Each entry has the identifying suffix (Local) or (Remote).

Select the source system from which you have replicated backups. PowerProtect Data Manager opens the remote view and presents a subset of the regular UI navigation tools:

- **Restore**
 - **Assets**— Shows replicated copies.
 - **Running Sessions**— Allows you to manage and monitor Instant Access sessions.
- **Alerts**— Shows alert information in a table, including audit logs.
- **Jobs**— Shows the status of any running restore jobs.

Each tool has the same function as for the local system. However, since the remote view is intended only for restore operations, the scope is limited to the replicated copies from the selected source system. While in remote view, a banner identifies the selected system.

 **NOTE:** For virtual machines, the quick recovery restore workflow does not include the **Restore VM Tags** option to restore vCenter tags and categories from the backup.

Use **Restore > Assets** to locate copies. The instructions for restoring each type of asset provide more information about restore operations.

When the recovery is complete, click **Remote Systems** and select the name of the local system to exit remote view.

Recover a failed PowerProtect Data Manager backup

Steps

1. Redeploy the PowerProtect Data Manager OVA.
2. Contact Customer Support.

Managing Alerts, Jobs, and Tasks


Topics:

- [Configure Alert Notifications](#)
- [View and manage alerts](#)
- [View and manage Audit Logs](#)
- [Monitoring jobs and tasks](#)
- [Restart a job or task manually](#)
- [Restart a job or task automatically](#)
- [Resume misfire jobs after a PowerProtect Data Manager update](#)
- [Cancel a job or task](#)
- [Exporting logs](#)

Configure Alert Notifications

The **Alert Notifications** window of the PowerProtect Data Manager UI enables you to configure email notifications for PowerProtect Data Manager alerts.

Steps

1. From the PowerProtect Data Manager UI left navigation pane, select **Alerts**, and then select the **Alert Notifications** tab. The **Alert Notifications** window appears with a table that displays the details for existing notifications.
2. Click **Add**.
The **Add Alert Notification** dialog appears.
 **NOTE:** The **Add** button is disabled until you set up the email server. To add an alert notification, set up the email server in **System Settings > Support > Email Setup**. [Set up the email server](#) on page 163 provides more information.
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 or alias to receive notifications. This field is required in order to create an alert notification. Separate multiple entries with 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 how often the notification email will be sent out. For example, you can set the duration to 60 minutes in order to send out a notification email every 60 minutes.
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 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. With the Administrator, Backup Administrator, Restore

Administrator, or User role, you can access the alerts from the **Alerts** window. However, only some of these roles can manage alerts.

Steps




1. From 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.
The **System** tab displays all alert types.
3. To view more details about a specific entry, click  next to the entry in the table.
4. For the following steps, log in to the PowerProtect Data Manager UI with an account that has the Administrator, Backup Administrator, or Restore Administrator role.
5. To acknowledge the alert, select the alerts and then click **Acknowledge**.
6. To add or edit a note for the alert, click **Add/Edit Note**, and when finished, click **Save**.
7. To export a report of alert information to a .CSV file which you can download for Excel, select an entry in the table and then click **Export**.

 **NOTE:** If you apply any filters in the table, exported alerts include only those alerts that satisfy the filter conditions.

View and manage Audit Logs

Audit logs enable you to view specific information about jobs that are initiated in PowerProtect Data Manager so that you can determine compliance to service level objectives. You can access the audit logs from the **Administration > Audit Logs** window.

Steps

1. From the PowerProtect Data Manager UI left navigation pane, select **Administration > Audit Logs**.
The **Audit Logs** window displays audit information in a table.
 2. (Optional) Sort and filter audit information:
 - To filter audits by **Audit Type**, **Changed By**, or **Object Changed**, click .
 - To sort audits by **Changed At**, **Audit Type**, **Changed By**, or **Object Changed**, click a column heading.
 - To filter audits based on a search string, type a keyword in the **Search** field.
 3. To view more details about a specific entry, click  next to the entry in the table.
 - Review the information for the audit log.
 - Optionally, add a note for this audit log in the **Notes** field.
 4. To export an audit log report to a .csv file which you can download as an Excel file, click **Export**.
-  **NOTE:** If you apply any filters in the table, exported audit logs include only those logs that satisfy the filter conditions.
5. To change the retention period for audit logs, click **Set Boundaries**, select the number of days from the **Days of Retention** menu, and then click **Save**.

Monitoring jobs and tasks

Use the **Protection Jobs** and **System Jobs** windows in the PowerProtect Data Manager UI to monitor the status of certain data protection, system, and maintenance jobs and to view details about failed, in progress, or recently completed jobs. To perform analysis or troubleshooting, you can view a detailed log of a failed job or task. Jobs are categorized as protection jobs or system jobs.

You can also view details for a job group and individual jobs and tasks. When you click the job ID next to the job entry, the **Job ID Summary** window displays the information for only this job group, job, or task, so that you can monitor the status of individual jobs and tasks, view job and task details, and perform certain operations on jobs and tasks.

Use the filtering and sorting options in each window to find specific jobs or tasks, and to organize the information that you see. [Filter, group, and sort jobs](#) on page 146 provides more information.

NOTE: The **Protection Jobs** and **System Jobs** windows have been optimized for a screen resolution of at least 1920 x 1080 pixels with 100% scaling. Display issues might occur for smaller screens. Set your screen resolution to at least 1920 x 1080 pixels with 100% scaling.

Monitor and view jobs

Use the **Protection jobs** and **System jobs** windows to monitor and view status information for PowerProtect Data Manager operations.

Protection jobs

To view protection jobs and job groups, from the PowerProtect Data Manager UI left navigation pane, select **Jobs > Protection Jobs**.

The **Protection Jobs** window opens to display a list of protection jobs and job groups.

Protection jobs include:

- Cloud Tier
- Cloud Protect
- Consolidated Cloud Snapshot Manager jobs

NOTE: This job type does not apply to SAP HANA databases.

- Export Reuse
- Protect
- Replicate
- Restore

For application assets, the **Protect**, **Restore**, and **Replicate** job types can be monitored at the host or individual asset level. For all other asset types, the **Protect** and **Replicate** job types can be monitored at the host or individual asset level.

System jobs

To view system jobs and job groups, from the PowerProtect Data Manager UI left navigation pane, select **Jobs > System Jobs**.

The **System Jobs** window opens to display a list of system jobs and job groups.

System jobs include:

- Config
- Console
- Delete
- Disaster Recovery
- Cloud Disaster Recovery
- Cloud Copy Recovery
- Discovery
- Manage
- Notify
- System
- Validate



System jobs can be monitored at the job group or job level.

Job information

The main **Protection Jobs** and **System Jobs** windows lists basic job information.

The following information is available in the **Protection Jobs** and **System Jobs** windows.

Table 31. Job information

Column	Description
Job ID	The unique and searchable identifier for the job.
Status	Indicates the current state of the job. A job can be in one of the following states: <ul style="list-style-type: none">• Success• Completed with Exceptions• Failed• Canceled• Unknown• Skipped• Running• Queued• Canceling
Description	Description of the job.
Policy Name	Name of the protection policy that started the job.
Assets	Number of individual assets or tasks within the job group.
Job Type	Type of protection job or system job.
Asset Type	Type of asset.
Start Time	Date and time that the job is scheduled to begin.
End Time	Date and time that this job completed. This column is not shown by default. To see a complete list of filtering and sorting columns, click  .
Duration	Overall duration of the job. This column is not shown by default. To see a complete list of filtering and sorting columns, click  .

View details for protection jobs

In the **Job ID Summary** window for protection jobs, you can view details and status of specific jobs. For application protection jobs, you can view details and status of specific jobs and assets. This information can be helpful when troubleshooting to determine whether one or more assets caused a job to fail.

Steps

1. From the PowerProtect Data Manager UI left navigation pane, select **Jobs > Protection Jobs**.
2. Click the job ID next to the job name.

The **Job ID Summary** window opens and lists all jobs as entries in the table.

You can filter, group, and sort the information that appears in the window. [Filter, group, and sort jobs](#) on page 146 provides more information.

The policy name, job type, and asset type appear at the top of the **Job ID Summary** window.

The overall job group metrics and details also appear, as shown in the following figure.

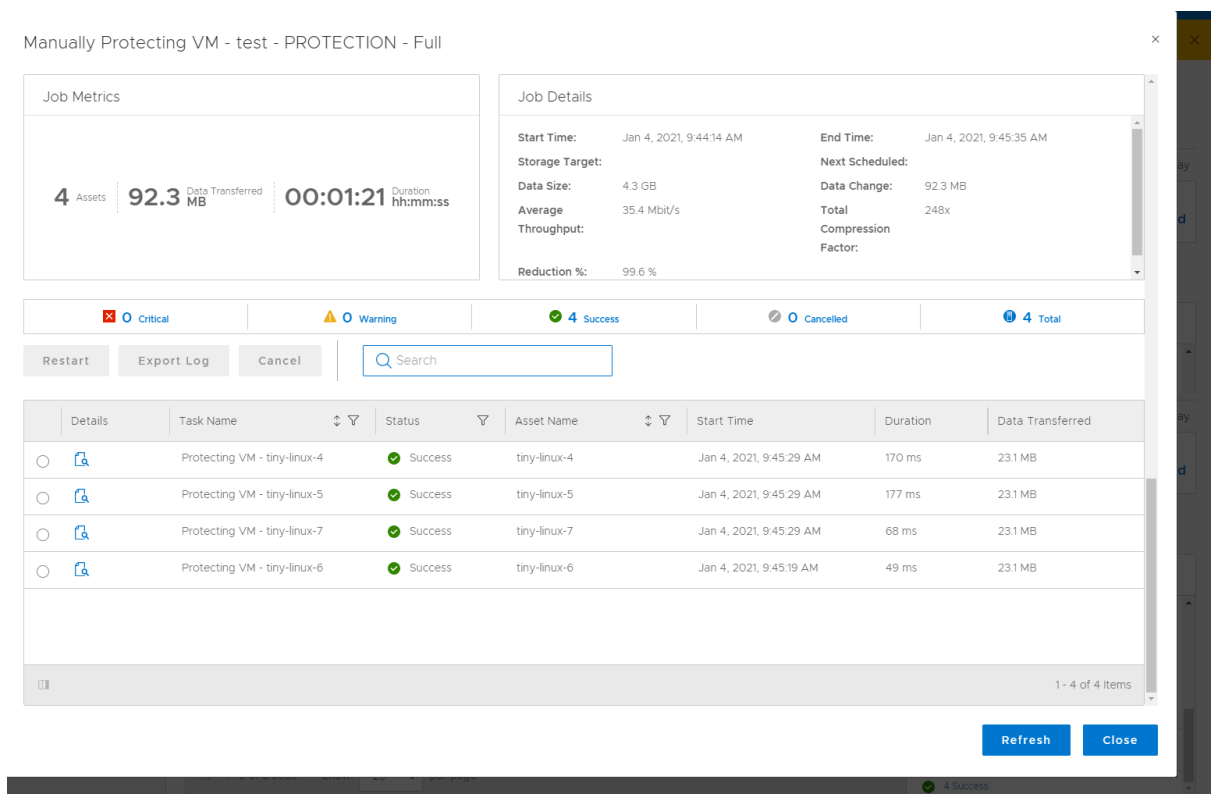


Figure 7. List of protection jobs

The **Job Metrics** section displays the number of assets, the total size of the data transferred, and the overall duration of the job group. The total duration of jobs within the job group will be shorter than the duration indicated in the Job Metrics.

The **Job Details** section displays more specific information such as the job start and end time, the protection storage target, the average data transfer rate, the amount of data changed since the last protection job, the average throughput, and the rate of compression applied. For restore jobs of SQL databases, some fields are either not applicable or set to zero.

Job metrics and details do not display or might be incomplete for job groups that contain the following:

- Application agent assets from a protection job that was performed for an application agent previous to version 19.7. To display the correct information for these assets, update the application agent on these assets to the current version.
- Oracle database assets.

Click **Hide Summary** to hide job metrics and details, or click **Show Summary** to view job metrics and details.

When you hover over a job, the **Job ID Summary** displays a message for the job to indicate its progress. Depending on the job and if any issues are detected, one of the following statuses is shown:

- No reported issues—No issues affecting the job.
- Timeout issues—Timeout issues might be affecting the job.
- Connectivity issues—Network connectivity issues might be affecting the job.
- Stats stall issues—Progress for this job is stalled.

The **Job ID Summary** window provides summary data for specific jobs and assets in a table view. For grouped assets, the host-level entry indicates the sum of the values of a given metric for every asset on the host.

The following table describes the columns that might appear in the window. Not all columns will appear in the **Job ID Summary** window of every asset type.

Table 32. Job ID Summary window details

Column	Description
Details	Click in the Details column to view job statistics and summary information.
Asset	Name of the job for the asset.
Status	Indicates the current state of the job. A job can be in one of the following states:

Table 32. Job ID Summary window details (continued)

Column	Description
	<ul style="list-style-type: none"> • Success • Completed with Exceptions • Failed • Canceled • Unknown • Skipped • Running • Queued • Canceling
Size	Size of job for the asset.
Data Transferred	Total data that is transferred to storage.
Reduction %	Total reduction percentage of storage capacity for the job.
Start Time	Date and time that the job is scheduled to begin.
End Time	Date and time that this job completed.
Error Code	If the job did not successfully complete, a numeric error code appears. To view a detailed explanation, double-click the error code.
Host/Cluster/Group Name	The hostname, cluster, or group name that is associated with the asset.
Duration	Overall duration of the job. This column only appears for Protect and Replicate job types for application assets.
Asset Size	Total size of the asset in bytes.
Data Compressed	Capacity that is used after client compression of the data in bytes. This column only appears for Protect and Replicate job types for application assets.
Download log	Detailed log for an asset or task that you can export and download.

- To view job details and summary information, click  in the **Details** column next to the job, or expand the entry for the job group by clicking .

For grouped assets, the **Job ID Summary** window lists the individual jobs for each asset within the job group.

The right pane appears and displays the following information about the job or task:

- **Step Log**—Displays a list of steps that have been completed for the job or task, and indicates the amount of time that was required to complete each step.
- **Details**—Displays statistics and summary information, such as the start time and end time, asset size, duration, and so forth.
- **Error**—Displays error details for failed jobs.
- **Canceled**—Displays details for canceled jobs.
- **Skipped**—Displays details for skipped jobs.
- **Unknown**—Displays details for jobs with an unknown status.

View details for system jobs and tasks

In the **Job ID Summary** window for system jobs, you can view details and status of specific jobs and tasks. This information can be helpful when troubleshooting to determine whether one or more jobs or tasks caused a job to fail.

Steps

- From the PowerProtect Data Manager UI left navigation pane, select **Jobs > System Jobs**.
- Click the job ID next to the job name.

The **Job ID Summary** window opens to display a list of all system jobs or tasks.

You can filter, group, and sort the information that appears in the window. [Filter, group, and sort jobs](#) on page 146 provides more information.


For jobs and tasks, a table appears at the bottom of the window. The success or failure of individual tasks is indicated in the **Status** column. If a failed job or task requires action, a status of **Critical** appears.

When you hover over a job or task, the **Job ID Summary** displays a message for the job to indicate its progress. Depending on the job and if any issues are detected, one of the following statuses is shown:

- **No reported issues**—No issues affecting the job.
- **Timeout issues**—Timeout issues might be affecting the job.
- **Connectivity issues**—Network connectivity issues might be affecting the job.
- **Stats stall issues**—Progress for this job is stalled.

The **Job ID Summary** window provides summary data for specific jobs and tasks in a table view. The following table describes the columns that might appear in the window. Not all columns will appear in the **Job ID Summary** window of every asset type.

Table 33. Job ID Summary window details

Column	Description
Details	Click  in the Details column to view job or task statistics and summary information.
Task Name	Name of the task.
Status	Indicates the current state of the job or task. A job or task can be in one of the following states: <ul style="list-style-type: none"> • Success • Completed with Exceptions • Failed • Canceled • Unknown • Skipped • Running • Queued • Canceling
Asset	Name of the asset.
Start Time	Date and time that the job or task is scheduled to begin.
Duration	Overall duration of the job or task.
Data Transferred	Total data that is transferred to storage.

3. To view job or task details and summary information, click  in the **Details** column next to the individual job or task.

The right pane appears and displays the following information about the job or task:

- **Step Log**—Displays a list of steps that have been completed for the job or task and indicates the amount of time that was required to complete each step.
- **Details**—Displays statistics and summary information, such as the start time and end time, asset size, duration, and so forth.
- **Error**—Displays error details for failed jobs.
- **Canceled**—Displays details for canceled jobs.
- **Skipped**—Displays details for skipped jobs.
- **Unknown**—Displays details for jobs with an unknown status.

Filter, group, and sort jobs

The **Protection Jobs** and **System Jobs** windows provide options to filter, group, and sort the information that appears. Select a job to display its **Job ID Summary** window.

Filter jobs by status

Use the quick filters at the top of the window to filter jobs by status. By default, all jobs are shown regardless of status. To display only jobs with a specific status, at the top of the window, select one of the following options:

- **Failed**
- **Completed with Exceptions**
- **Success**
- **Canceled**
- **In Progress**
- **Completed**

In Progress jobs include **Running**, **Queued**, and **Canceling** jobs.

When you select a quick filter to filter jobs by a certain status, the window displays the filter above the table. To stop filtering by the selected status, click **x**.

Filter jobs by start time

Use the **Start Time** filter to display jobs that started in a specified period. Select from one of the following options:

- All jobs
- Last 24 hours
- Last 3 days
- Last 7 days
- Last 30 days
- Specific date
- Custom date range

Group jobs

The **Group by** feature in the **Job ID Summary** window provides options to group assets within a protection job.

The following asset types support the **Group by** feature:

- Microsoft SQL and Exchange databases
- Oracle databases
- File Systems
- SAP HANA databases
- Kubernetes clusters
- Network attached storage (NAS) shares
- VMware Virtual Machines

To group assets in a protection job, in the **Job ID Summary** window for the job, select an option from the **Group By** drop-down list. To display all assets, select **Group by > None**. For example, to group virtual machine assets by ESX host, click **Group by > ESX Host**.


The following table lists the available **Group by** options:

Table 34. Group by options

Asset type	Options
Microsoft SQL database	SQL Host
	SQL Instance
Oracle database	Oracle Host

Table 34. Group by options (continued)


Asset type	Options
	Oracle Instance
File System	File System Host
	File System Host OS
Microsoft Exchange database	Exchange Host
SAP HANA database	SAP HANA Host
Kubernetes	Kubernetes Cluster
	Kubernetes Namespace
NAS	NAS Server
	NAS Appliance
VMware Virtual Machine	Datastore
	ESX Host
	Virtual Datacenter
	VM Guest OS
	VMware Cluster

 **NOTE:** Currently, the **Group by** filter is only available for the **Protect** job types.

Search filter

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.

Filter and sort information in tables

You can filter and sort the information that appears in table columns. Click  in the column heading to filter the information in a table column, or click a table column heading to sort that column.

To see a complete list of filtering and sorting columns, click . Depending on the type of job, the available filtering and sorting columns might differ.

The following filtering and sorting options are available for jobs and tasks:

Table 35. Protection and System Jobs windows

Filtering options	Sorting options
Filter jobs or tasks by Job ID , Status , Description , Policy Name , Job Type , End Time , and Asset Type .	Sort jobs or tasks by Job ID , Description , Policy Name , Job Type , Asset Type , Start Time , and End Time .

Table 36. Job ID Summary window for protection jobs


Filtering options	Sorting options
Filter jobs by Asset , Status , Error Code , Start Time , or End Time . For application assets, you can also filter jobs by Host/Cluster/Group Name .	Sort jobs by Asset , Status , Error Code , Size , Data Transferred , Reduction % , Start Time , End Time , or Duration . For application assets, you can also sort jobs by Host/Cluster/Group Name .
 NOTE: For application assets, these options are only available when you select Group by > None .	

Table 36. Job ID Summary window for protection jobs


Filtering options	Sorting options
	 NOTE: For application assets, these options are only available when you select Group by > None .

Table 37. Job ID Summary window for system jobs

Filtering options	Sorting options
Filter jobs or tasks by Task Name , Status , Asset , or Start Time .	Sort jobs or tasks by Task Name , Status , Asset , Start Time , Duration , or Data Transferred .

Restart a job or task manually

You can manually restart a failed virtual machine backup.

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 canceled and cannot be restarted.
- Cloud Native Entity jobs cannot be restarted.

Steps

1. From the PowerProtect Data Manager UI left navigation pane, select **Jobs > Protection Jobs** or **Jobs > System Jobs**. The **Protection Jobs** or **Systems Jobs** window appears, displaying all completed and running jobs.
2. To restart a failed job or job group, select the failed job or job group from the list, and then click **Restart**.
3. To restart a failed job or task from the **Job ID Summary** window:
 - a. Click the job ID next to the name of the job or job group.
The **Job ID Summary** window opens to display a list of all jobs or tasks.
 - b. Select the job or task from the list, and then click **Restart**.

Results

After the job or task has been restarted, the status indicates **Running** or **Queued**.

Restart a job or task automatically

If a backup job fails or one of the tasks within the job fails, you can enable automatic restart of the failure by configuring auto retry in the `entrypoint.sh` file. Auto retry can be useful in situations where the failure is due to an intermittent issue, such as a network or service interruption.

Prerequisites

In PowerProtect Data Manager, some services that are required for auto retry, such as the workflow service, have been moved into a docker container. In order to enable auto retry, ensure that the workflow service is running in a docker.

About this task

Auto retry is only supported for daily, weekly, or monthly schedules for virtual machine and File System agent protection operations.

Steps

1. Log in to the PowerProtect Data Manager server by using SSH.

2. Copy the `entrypoint.sh` file from the workflow container by typing the following:

```
docker cp workflow:/workflow/bin/entrypoint.sh .
```

3. Configure auto retry by adding a line to `entrypoint.sh`:

- a. Type **`vi entrypoint.sh`**

- b. Before the last line in the output, `-jar /${APP_NAME}/lib/workflow-manager.jar`, add the following:

```
-Denable.auto.retry.scheduler=true \
```

NOTE: Auto retry is disabled by default. After adding this line, if you want to disable this setting at any point, change the entry to **`-Denable.auto.retry.scheduler=false \`**

4. Optionally, add the following application properties to the file to specify a maximum number of auto retries and a time interval at which subsequent auto retry attempts will occur:

```
-Dfailed.job.retry.max.count=2 \
```

```
-Dfailed.job.retry.interval=PT30M \
```

NOTE: The values specified above are the recommended default values. Auto retries will only occur during the activity window. If you perform a manual retry in the PowerProtect Data Manager UI, this retry will not count towards the auto retry max count.

For the interval duration, the value must be specified in ISO-8601 format.

5. Save the `entrypoint.sh` file to the workflow container by typing the following:

```
docker cp entrypoint.sh workflow:/workflow/bin/
```

6. Restart the workflow service by using one of the following methods:

- Type **`docker container restart workflow`**

NOTE: For the configuration to be applied successfully using this method, you can only restart the container. If you restart your workflow service or your PowerProtect Data Manager operating system, the configuration will be lost.

- Type the following to save the docker image and restart the workflow service. For example:

```
docker commit workflow dpd/ppdm/ppdmc-workflow:PowerProtect Data Manager version  
workflow restart
```

where *PowerProtect Data Manager version* is the PowerProtect Data Manager version that is deployed on your system.

You can use this method to permanently apply the configuration change after restoring the docker image.

Results

Upon configuration, the workflow service is scheduled to run every 30 minutes to determine if any jobs or tasks have failed. If a restart occurred, the status will indicate **Running** or **Queued**. To view whether a failed job or task has been restarted, go to the **Jobs** window in the PowerProtect Data Manager UI and select **Running** or **Queued**.

Resume misfire jobs after a PowerProtect Data Manager update

During an update, the PowerProtect Data Manager system enters maintenance mode. Any job that is not in queue and is scheduled to run during the time that the PowerProtect Data Manager system is in maintenance mode will be missed. These missed jobs are known as misfires. As of this release, PowerProtect Data Manager uses the Quartz Scheduler to resume scheduled workflows when the service recovers or when the schedule resumes.

About this task

The trigger and firing data of jobs are stored in a PostgreSQL database application. If the schedule service is down, such as during an update, the Quartz Scheduler recovers this data and resumes the jobs when the PowerProtect Data Manager system is operational again.

NOTE: In the current release, this feature is enabled by default.

You can enable or disable the misfire feature by configuring the `entrypoint.sh` file.

Steps

1. Log in to the PowerProtect Data Manager server by using SSH.
2. Copy the `entrypoint.sh` file from the scheduler container by typing the following:

```
docker cp scheduler:/scheduler/bin/entrypoint.sh .
```

3. Configure the misfire conditions in the `entrypoint.sh` file:

NOTE: Before the last line in the output, `-jar /${APP_NAME}/lib/scheduler-core.jar`), add the lines for each misfire condition.

- a. To enable misfire and trigger each job once, add the following properties and corresponding values:

```
-Dspring.quartz.properties.misfire.cron.strategy=WITH_MISFIRE_HANDLING_INSTRUCTION_FIRE_AND_PROCEED \
```

NOTE: This condition is enabled by default.

```
-Dspring.quartz.properties.misfire.calendar.strategy=WITH_MISFIRE_HANDLING_INSTRUCTION_FIRE_AND_PROCEED \
```

- b. To enable misfire and trigger each job as many times as misfire happens, add the following properties and corresponding values:

```
-Dspring.quartz.properties.misfire.cron.strategy=WITH_MISFIRE_HANDLING_INSTRUCTION_IGNORE_MISFIRES \
```

```
-Dspring.quartz.properties.misfire.calendar.strategy=WITH_MISFIRE_HANDLING_INSTRUCTION_IGNORE_MISFIRES \
```

- c. To disable misfire, add the following properties and corresponding values:

```
-Dspring.quartz.properties.misfire.cron.strategy=WITH_MISFIRE_HANDLING_INSTRUCTION_DO_NOTHING \
```

```
-Dspring.quartz.properties.misfire.calendar.strategy=WITH_MISFIRE_HANDLING_INSTRUCTION_DO_NOTHING \
```

4. Save the `entrypoint.sh` file to the scheduler container by typing the following:

```
docker cp entrypoint.sh scheduler:/scheduler/bin/
```

5. Restart the scheduler service by using one of the following methods:

- Type **`docker container restart scheduler`**

NOTE: For the configuration to be applied successfully using this method, you can only restart the container. If you restart your scheduler service or your PowerProtect Data Manager operating system, the configuration will be lost.

- Type the following to save the docker image and restart the scheduler service:

```
docker commit scheduler dpd/ppdm/ppdmc-scheduler:PowerProtect Data Manager version  
scheduler restart
```

where *PowerProtect Data Manager version* is the PowerProtect Data Manager version that is deployed on your system.

You can use this method to permanently apply the configuration change after restoring the docker image.

NOTE: Ensure that the PowerProtect Data Manager version specified in the `commit` command matches the PowerProtect Data Manager version that is deployed on your system.

Cancel a job or task

From the PowerProtect Data Manager UI, you can cancel a backup or restore 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 available for the following supported jobs and tasks only:


- Backup and restore of:
 - Virtual machine

- Kubernetes
- NAS
- File System agent
- SQL agent
- Server DR
- Cloud DR
- Backup (only) of:
 - Exchange agent
 - Oracle agent
 - SAP HANA agent
- Replication
- Compliance
 - Copy deletion
 - Compliance verification
 - Auto promotion to full backup
 - Cleaning MTree or deleting user
 - On-demand update retention
- Support
 - Communication of telemetry data
 - Export of job and job group logs
 - Adding log bundles

Steps

1. From the PowerProtect Data Manager UI left navigation pane, select **Jobs > Protection Jobs** or **Jobs > System Jobs**. The **Protection Jobs** or **Systems Jobs** window appears, displaying all completed and running jobs.

2. To cancel a job or job group, select a job or job group 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.


The **Protection Jobs** or **System Jobs** window displays the status of the canceled job or job group. 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**.

3. To cancel an individual job or task from the **Job ID Summary** window:

- a. Click the job ID next to the name of the job or job group.

The **Job ID Summary** window opens to display a list of all jobs or tasks.

- b. Select a job or task that is in-progress, and then click **Cancel**.


 **NOTE:** If a job or task is almost complete, the cancellation might fail. If the cancellation fails, a message displays indicating that the task cannot be canceled.

- c. Click **Close**.

The **Job ID Summary** 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**.

Exporting logs

The PowerProtect Data Manager UI enables you to export and download a detailed log of a job, asset, or task to perform analysis or troubleshooting.


You can export and download a log for a job, asset, or task with any status. After you export a log, you can download it by clicking .

Export logs for jobs

You can export and download a log for a protection job or system job.

Steps

1. From the PowerProtect Data Manager UI left navigation pane, select **Jobs > Protection Jobs** or **Jobs > System Jobs**.
The **Protection Jobs** or **Systems Jobs** window appears, displaying all jobs.
2. Select a job from the list, and then click **Export Log**.

 indicates the log export operation is in progress, and is shown next to the asset or task in the **Download Log** column. Hover over the icon to display the progress. When the log export is complete, you can download the log.


3. Click  next to the ID for the job to download the exported log.

Export logs for assets or tasks

You can export and download a log for an individual asset or task.

Steps

1. From the PowerProtect Data Manager UI left navigation pane, select **Jobs > Protection Jobs** or **Jobs > System Jobs**.
The **Protection Jobs** or **Systems Jobs** window appears, displaying all jobs.
2. Click the job ID next to the name of the job.
The **Job ID Summary** window opens.
3. Select the asset or task from the list, and then click **Export Log**.

 indicates the log export operation is in progress, and is shown next to the asset or task in the **Download Log** column. Hover over the icon to display the progress. When the log export is complete, you can download the log.

4. Click  in the **Download Log** column to download the exported log.


Modifying the System Settings

Topics:

- [System settings](#)
- [System Support](#)
- [Modifying the PowerProtect Data Manager virtual machine disk settings](#)
- [Memory optimization](#)
- [Configure the DD system](#)
- [Virtual networks \(VLANs\)](#)

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 change the IP address of the PowerProtect Data Manager appliance, or modify other network settings such as the hostname, subnet mask, gateway, or DNS servers.

Prerequisites

 **NOTE:** When you change the IP address or hostname, the system becomes unavailable until all components are restarted.


Steps

1. From the PowerProtect Data Manager UI, click , select **System**, and then click **Network**.
2. Update the fields as necessary:
 - **Hostname**
 - **IP Address**
 - **Subnet Mask**
 - **Gateway**
 - **Primary DNS**
 - **Secondary DNS**
3. Click **Save**.

Synchronize time on PowerProtect Data Manager and other systems

The PowerProtect Data Manager system time is synchronized with the ESXi host system.


The PowerProtect Data Manager system time must match the systems with which it interfaces or compliance check will fail. Dell EMC recommends that all systems be configured to use an NTP server.

 **NOTE:** Times in the UI are always displayed as local to the users time zone based on their browser or system settings. The PowerProtect Data Manager system might be in a different time zone but when viewing the UI it will always show the times local to the user.

Modify the appliance time zone

Use this procedure to modify the time zone for the PowerProtect Data Manager appliance.

Steps

1. From the PowerProtect Data Manager UI, click , select **System**, and then click **Timezone**.
2. From the **Timezone** list, select the applicable time zone.
3. Click **Save**.

Enable replication encryption


You can ensure that replicated content is encrypted while in-flight to the destination storage, and then decrypted before it is saved on the destination storage.

About this task

The encryption settings on both the source and destination systems must match to ensure successful replication.


For example, if you enable in-flight encryption in PowerProtect Data Manager, the setting must be 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 that were initiated during the period when the source and destination server encryption settings did not match will fail.

Steps

1. From the PowerProtect Data Manager UI, click , and then select **Security**.
The **Security** dialog box appears.
2. Click the **Replication Encryption** switch so it is enabled, and then click **Save**.

Next steps

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 DDOS version 6.2 and earlier installed, the status might display as `Unknown`. DDOS version 6.3 and later supports authentication mode. DDOS 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 DD systems by using **DD System Manager**, as described in the *DDOS Administration Guide*.

Backup and restore encryption

You can encrypt backup or restore data that is in transit for centralized and self-service operations with DD Boost encryption, using TLS. Encryption of backup and restore data in-flight is available for application assets and NAS assets only.

By default, PowerProtect Data Manager supports an encryption strength of `HIGH` and uses DD Boost anonymous authentication mode. The DD Boost encryption software uses the **ADH-AES256-SHA** cipher suite. The *DD Boost for OpenStorage Administration Guide* provides more information about the cipher suite for high encryption.

The following table lists the workloads and operations that support encryption of data in-flight:


 **NOTE:** Refer to the agent user guides for more information about the centralized and self-service operations that are supported.


Table 38. Supported workloads

Workload	Centralized backup	Centralized restore	Self-service backup	Self-service restore
File System with Application Direct	Yes	Yes (image-level restore only)	Yes	Yes (image-level restore only)
Microsoft SQL with Application Direct	Yes	Yes (database-level restore only)	Yes	Yes (database-level restore only)
Microsoft Exchange with Application Direct	Yes	N/A	Yes	Yes
Oracle with Application Direct	Yes	N/A	Yes	Yes
SAP HANA with Application Direct	Yes	N/A	Yes	Yes
Network attached storage (NAS)	Yes	Yes	N/A	N/A

Enabling encryption imposes additional overhead. Backup and restore performance for any client could be affected by 5-20% with encryption enabled.

You can enable or disable backup and restore encryption in the PowerProtect Data Manager UI.

PowerProtect Data Manager supports backup and restore encryption for all supported DD Boost and DDOS versions. The most up-to-date software compatibility information for PowerProtect Data Manager is provided in the [eLab Navigator](#).

 **NOTE:** You do not need to enable in-flight encryption on connected DD systems. If DD encryption settings exist, the higher setting takes precedence.

Enable backup and restore encryption

You can ensure that the backup and restore content is encrypted when read on the source system, transmitted in encrypted form, and then decrypted before it is saved on the destination storage.

Prerequisites


Review the information in [Backup and restore encryption](#) on page 154 to learn more about backup and restore encryption.

The encryption settings determine if the data transfer is encrypted while in-flight during backup and restore operations.

- For SQL, Exchange, File System, SAP HANA, and Oracle workloads, backup and restore encryption is only supported for Application Direct hosts.
- When a new host is added to PowerProtect Data Manager, host configuration is run to push the encryption settings to the host.
- Only hosts that have PowerProtect Data Manager 19.9 application agents installed support the host configuration.


About this task

Steps

1. From the PowerProtect Data Manager UI, click , and then select **Security**.
The **Security** dialog box appears.
2. Click the **Backup/Restore Encryption** switch so it is enabled, and then click **Save**.

Next steps

The **Jobs > System Job** window of the PowerProtect Data Manager UI creates a job to enable protection encryption. This job pushes encryption settings to the hosts to be used for self-service operations. Within the system job, a host configuration job is created for each host. If an error occurs, you can retry the system job or individual host configuration job.

 **NOTE:** For centralized backup and restore operations, PowerProtect Data Manager sends the encryption settings to the application agents on the Application Direct hosts and network attached storage (NAS).

You can disable encryption for backup and restore content by clicking the **Backup/Restore Encryption** switch. PowerProtect Data Manager creates a system job in the **Jobs > System Job** window to disable protection encryption.

Additional considerations

Review the following additional considerations for backup and restore encryption.

To validate whether encryption is being used, you can check the status of existing connections on the DD system by running the `ddboost show connections` command in the DD Boost CLI:

- The value in the **Encrypted** column is set to *Yes* if a connection has been established with encryption.
- If a client establishes a connection with encryption, and establishes another connection without encryption, the value in the **Encrypted** column is set to *Mixed*. This might occur for one of the following reasons:
 - Encryption settings that are defined on a per-client basis remain in place for a while after the client has disconnected. If the client previously established a connection without encryption and then later established a connection with encryption, the value shows as *Mixed*.
 - Encryption settings are not specified for the DD Boost connections that are created on the application agent. Refer to the individual user guides for more information.
- If encryption settings exist on the DD and are also enabled in PowerProtect Data Manager, the higher encryption setting takes precedence. As a result, the **Encrypted** column will always show *Mixed* or *Yes*.

PowerProtect Data Manager licensing

PowerProtect Data Manager can be licensed in several different ways. This section describes the different types of available licenses and how to install a license.

For more information about licensing, see the *PowerProtect Data Manager Licensing Guide*.

License types

There are several different types of licenses, and they can provide licensing for different periods of time.

The available license types are described in the following table.

Table 39. License types

License type	Description
Trial	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 that you can apply a permanent license.
Front-end protected capacity by terabyte (FETB)	The primary model of eLicensing, which is based on the 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 data.
Socket-based	Licensed per CPU socket on virtual machine hosts that are being backed up or replicated.

Perpetual and term-based (subscription) licenses

Licensed software is offered in perpetual and term-based licenses. Your quote identifies 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 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.

Add a license

You can add a license file to PowerProtect Data Manager and view license details, such as capacity usage and software ID number.

Prerequisites


To obtain the XML license file from the Dell EMC license management website, you must have the License Authorization Code (LAC), which is emailed from Dell EMC. If you have not received the LAC, contact your technical support professional.

About this task

To review existing license information, go to **Settings > License**.

To add a license, perform the following steps:

Steps

1. From the PowerProtect Data Manager user interface, click , and then select **License**.
2. On the **License** window, perform one of the following actions:
 - Copy and paste the text from the license file into the text box.
 - Click **Upload File**, browse to the location of the license file and select the file, and then click **Open**.
The license file content appears in the **License** window.
3. Click **Save**.

Results

A message appears in the **License** window to confirm that the license is successfully added.

Specify a vCenter Server as the PowerProtect Data Manager host

PowerProtect Data Manager provides an option to identify a vCenter Server as the host vCenter.

About this task


When a vCenter Server is marked as the vCenter that hosts PowerProtect Data Manager, you can use this vCenter for the following operations:

- Performing system activities, such as virtual machine-level configuration.
- Performing software updates in circumstances that require taking a PowerProtect Data Manager snapshot.
- Enabling Cloud Disaster Recovery (CDR), in order to increase the PowerProtect Data Manager CPU and memory that is required for these operations. A vCenter host is a prerequisite for CDR, as specified in the **Cloud Disaster Recovery** tab of the PowerProtect Data Manager UI **Infrastructure > Asset Sources** window.

To specify a vCenter Server as the vCenter that hosts PowerProtect Data Manager, you can:

- Add and discover this vCenter as an asset source in the PowerProtect Data Manager UI **Infrastructure > Asset Sources** window, or
- Enter the vCenter Server information in the **Hosting vCenter** window, as outlined in the following procedure.


Steps

1. From the PowerProtect Data Manager UI, click , and then select **Hosting vCenter**.
The **Hosting vCenter** window appears.
2. Choose from one of the following options:

- **Enter FQDN/IP**—Select this option to manually enter the fully qualified domain name or IP of the vCenter, the port number, and to select the vCenter **Host Credentials**. The **Host Credentials** list is populated with vCenter Servers that have already been added and discovered in PowerProtect Data Manager. If the host vCenter credentials do not appear in the list, select **Add Credentials** to enter this information.
- **Select FQDN/IP from asset sources**—Select this option to obtain the host vCenter Server information automatically from a vCenter asset source that has already been added and discovered in PowerProtect Data Manager.

3. Click **Save**.

Results

If the host vCenter Server is added as an asset source in PowerProtect Data Manager, a  icon displays next to this vCenter in the **Infrastructure > Asset Sources** window.

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 , and then select **Support**.

Configuring SupportAssist for PowerProtect Data Manager

SupportAssist is a support tool that communicates with PowerProtect Data Manager to monitor your environment, automatically detect current and potential issues, and collect and store diagnostic data. SupportAssist securely sends the data that is required for troubleshooting an issue to Technical Support for diagnostic purposes and customer support.

SupportAssist is at heart of the connectivity platform as a unified communication point between PowerProtect Data Manager and Technical Support.

SupportAssist provides the following features and benefits:

- Proactive monitoring and issue prevention
- Facilitates update package downloads
- Automatic support case creation based on event alerting
- Automatic health checks
- Communicates telemetry data
- Real-time troubleshooting
- Customer support

Configure SupportAssist to receive automated support capabilities for your PowerProtect Data Manager system.

Migrating to SupportAssist

SupportAssist provides automated support capabilities for PowerProtect Data Manager systems. SupportAssist replaces Secure Remote Services (SRS) in this release of PowerProtect Data Manager

If you have configured SRS previously, the PowerProtect Data Manager system automatically migrates SRS to SupportAssist when you update PowerProtect Data Manager.

If you do not have SRS configured, you can configure SupportAssist directly.

Use the following procedures to configure SupportAssist.


Generate SupportAssist access key and PIN

An access key and PIN are required to configure a secure connection between PowerProtect Data Manager and SupportAssist. You only need to apply the access key and PIN once.

About this task

Use the following procedure to generate your SupportAssist access key and PIN:

Steps

1. Go to the [Customer Support](#) website and log in to your account.
 2. In the search box, type PowerProtect Data Manager and click **Search**.
 3. Click **Generate Access Key** in the **Quick links** pane.
 4. Enter the product ID (serial number) in the search box.
 5. In the **Create PIN** field, enter a 4-digit PIN.
Record the PIN for later use.
 6. Click **Generate Access Key**.
The access key is sent to the email address for your account.
-  **NOTE:** It might take up to 5 minutes to receive the access key in your email.



Connect to the SupportAssist Enterprise

Establish a connection to the SupportAssist Enterprise to ensure access to Technical Support. SupportAssist enables you to connect PowerProtect Data Manager directly or through a gateway server.

Prerequisites

- Apply a valid PowerProtect Data Manager license.
- If you are connecting through the gateway server, the SRS gateway version must be 3.40 or later.
- Apply a valid access key and PIN.
- HTTPS port 443 of *esrs3-core.emc.com* and *esrs3-core.dr.emc.com* is not blocked by the network firewall.

Steps

1. From the PowerProtect Data Manager UI, click , select **Support**, and then click **SupportAssist**.
The **Support** window opens to the **SupportAssist** page.
2. On the **Connection** tab, click **Connect Now**.
3. Select one of the following options:
 - **Connect Directly**
Select this option to connect PowerProtect Data Manager directly, and then enter the SupportAssist Access Key and PIN.
 **NOTE:** Remote Support functionality is currently not supported for PowerProtect Data Manager systems using a direct connection.
 - **Connect via Gateway**
Select this option to connect PowerProtect Data Manager through a gateway server, and then perform the following tasks.
 - a. Enter the SupportAssist gateway server IP address and port number.
 - b. Click **Test** to test the connection to the gateway server.

Wait until the connection test is complete. If the connection is successful, a green check mark is displayed next to the gateway IP address and port number.
 - c. Enter the SupportAssist Access Key and PIN.
4. Click **Enable Connect**.


Results

PowerProtect Data Manager is connected to the SupportAssist Enterprise.

Update or configure contact data

Provide contact information for the person that Technical Support will contact with diagnostic reports. You can add or update contact data for SupportAssist at any time.

Steps

1. From the PowerProtect Data Manager UI, click , select **Support**, and then click **SupportAssist**. The **Support** window opens to the **SupportAssist** page.
2. Select the **Contacts** tab.
3. To add a primary contact, complete the following steps:
 - a. Enter the following information:
 - **First Name**
 - **Last Name**
 - **Email**
 - **Phone**
 - b. Select the **Preferred Language** from the list.
 - c. Click **Save**.
4. To add a secondary contact, click **+ Add Secondary Contact** and enter the required information.


Add AutoSupport

When AutoSupport is enabled, automated support information, telemetry reports, alert summaries, and CloudIQ reports are sent.

About this task

If SupportAssist and SMTP are both configured, this information is sent using the option that you choose in the **System Settings > Support > AutoSupport** window.


Steps

1. From the PowerProtect Data Manager UI, click , select **Support**, and then click **AutoSupport**. The **AutoSupport** window appears.
2. Change the `Enable AutoSupport` option to **Disabled** or **Enabled**, and click **Save**.

When you enable AutoSupport, select whether to receive the AutoSupport communications through SupportAssist or email server.

When you enable AutoSupport, 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 AutoSupport, PowerProtect Data Manager stops sending error and telemetry data to SupportAssist or the SMTP server. PowerProtect Data Manager continues to send information for updates and other information.

 **NOTE:** To disable SupportAssist, clear the SupportAssist option in the AutoSupport window.

Change SupportAssist connection settings

Use the following procedure to change SupportAssist connection settings.

Steps

1. From the PowerProtect Data Manager UI, click , select **Support**, and then click **SupportAssist**.

The **Support** window opens to the **SupportAssist** page.

2. Select one of the following connection options:


- **Connect Directly**
- **Connect via Gateway**

To add a new gateway connection, complete the following steps:

- a. Enter the gateway IP address and port number.
- b. Click **Test**.

Wait until the connection test is complete. If the connection is successful, a green check mark is displayed next to the gateway IP address and port number.

3. Enter the SupportAssist Access Key and PIN.


 **NOTE:** If you are not connecting with a new access key, skip this step.

4. Click **Reconnect**.

Enable or disable SupportAssist

Enable the SupportAssist feature to automatically detect issues and collect diagnostic and usage data. You can also disable SupportAssist at any time.

Steps

1. From the PowerProtect Data Manager UI, click , select **Support**, and then click **SupportAssist**. The **Support** window opens to the **SupportAssist** page.
2. To enable SupportAssist, move the **Connect to SupportAssist** slider to the right. To disable SupportAssist, move the **Connect to SupportAssist** slider to the left.
The operation might take up to 5 minutes to complete.

Troubleshooting SupportAssist

Review the following information that is related to troubleshooting SupportAssist.

Failed to establish a SupportAssist connection

If you are connecting to SupportAssist with an access key and PIN that is already in use, the connection fails with error:

`Connection is failed: Get universalkey error: Access Key and Pin used`

If this issue occurs, obtain a new access key and PIN from [Dell EMC Support. Generate SupportAssist access key and PIN](#) on page 159 provides instructions.

The following error might display if the SWID is not added to the PowerProtect Data Manager back-end: `Connection is failed: Get universalkey error: Invalid Access Key and Pin`

If this issue occurs, contact Customer Support and ask them to check whether the SWID has been added to the PowerProtect Data Manager back-end.

Test gateway connection failed

If the Secure Remote Services (SRS) gateway version is earlier than 3.40, the connection to the gateway might fail. If you are using a gateway version that is earlier than 3.40, the SRS gateway configuration is not transferred to SupportAssist after updating PowerProtect Data Manager.

When updating PowerProtect Data Manager, the precheck dialog box displays a warning indicating that the SRS gateway version in use is earlier than 3.40, and to update the SRS gateway to the compatible version.

If you are using a gateway version earlier than 3.40, the update fails with the following error:

SYS0034

`Unable to upgrade from Secure Remote Services to SupportAssist.`

Details

The upgrade to SupportAssist is unsuccessful for one or more of the following reasons: 1) The SupportAssist service cannot start. 2) The gateway is not accessible. 3) An issue occurs during Gen3 key upgrade.

Recommended Action

In the PowerProtect Data Manager UI: 1) To open the Support dialog, click Settings and select Support. 2) In the left pane, select SupportAssist to set up SupportAssist.

If this issue occurs, perform the following:

1. Check that the gateway version is 3.40 or later.
2. Set up SupportAssist. In the PowerProtect Data Manager UI, click , select **Support**, and then click **SupportAssist**.

Connection status changes to "Not Connected"

If the connection status changes to "Not Connected":

1. Ensure that all prerequisites are met in [Connect to the SupportAssist Enterprise](#) on page 159.
2. If the issue persists, contact Customer Support.

Telemetry Collector

Telemetry Collector gathers information related to this system, including configuration, usage characteristics, performance, and deployment location information. Telemetry Collector manages remote access and the exchange of system data with Dell Inc. or its subsidiaries. The information that is gathered by Telemetry Collector is confidential and this data cannot be shared.

When you enable SupportAssist, you also enable Telemetry Collector, which allows Technical Support Engineers to collect data that is related to troubleshooting device and PowerProtect Data Manager software issues. Telemetry Collector does not collect any personal information.

Telemetry Collector populates three reports—a telemetry report, an alert summary report, and a CloudIQ report. Telemetry Collector collects details about the following objects:

- Cloud Data Recovery
- Asset Sources
- Hosts Information
- DD Inventory
- PowerProtect Data Manager operational inventory
- Integrated Storage
- Usage
- Licensing
- Compliance in last 24 hours
- Traffic Metrics
- Protection Policies
- Alerts
- Cloud Disaster Recovery metrics
- Service Level Agreement
- Assets
- Storage Systems
- Data targets
- Protection Details
- Compliance Details
- Audit logs
- Report Generated Time
- Update Summaries

CloudIQ reporting

When you enable AutoSupport, you also enable reporting. CloudIQ 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 CloudIQ includes configuration data, historical metrics and health score data.

Ensure that the following requirements are met:


- Add a valid license in **System Settings > License**.
- Set up SupportAssist in **System Settings > Support > SupportAssist**.
- Enable AutoSupport and select **SupportAssist**.

When AutoSupport is enabled, CloudIQ reports are sent automatically. To log in to CloudIQ, click the **Reporting** menu item, or go to <https://cloudiq.dell.com>. For more information on CloudIQ, refer to the CloudIQ Online Support site.

Set up the email server

The **Email Setup** page of the PowerProtect Data Manager **Support** window enables you to configure SMTP email server settings that control sending and receiving email related to resetting local user passwords and customizing alert notifications.

Steps

1. From the PowerProtect Data Manager UI, click , select **Support**, and then click **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 PowerProtect Data Manager AutoSupport email.
 - c. [Optional] **Recipient for Test Email:**
The email address to which you would like to send PowerProtect Data Manager test email.
 - d. [Optional] **Port:**
The default port is 25. PowerProtect Data Manager supports using non-default ports.
If the email setup is deleted, you must manually choose any non-default 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 AutoSupport

When AutoSupport is enabled, automated support information, telemetry reports, alert summaries, and CloudIQ reports are sent.

About this task

If SupportAssist and SMTP are both configured, this information is sent using the option that you choose in the **System Settings > Support > AutoSupport** window.

Steps

1. From the PowerProtect Data Manager UI, click , select **Support**, and then click **AutoSupport**.
The **AutoSupport** window appears.
2. Change the **Enable AutoSupport** option to **Disabled** or **Enabled**, and click **Save**.

When you enable AutoSupport, select whether to receive the AutoSupport communications through SupportAssist or email server.

When you enable AutoSupport, 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 AutoSupport, PowerProtect Data Manager stops sending error and telemetry data to SupportAssist or the SMTP server. PowerProtect Data Manager continues to send information for updates and other information.

 **NOTE:** To disable SupportAssist, clear the SupportAssist option in the AutoSupport window.

Enabling automatic update package checks and downloads


If SupportAssist is enabled, you can configure PowerProtect Data Manager to automatically check for update packages, and either alert you or automatically download them.

For more information about these options, see [Automatically check for an update package](#) on page 210


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.

Steps

1. From the PowerProtect Data Manager UI, click , select **Support**, and then click **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**, **VM Direct Engines**, or, if Cloud DR is deployed, **CDRS**), set the log bundle duration, and click **Save**.
The **Jobs** window displays the progress of the log bundle creation. Also, 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 in the **Bundle Name** column.

Audit logging and monitoring system activity

The Linux audit daemon (`auditd`) tracks and logs security-relevant events on the PowerProtect Data Manager system.

Users with the Administrator role can use `auditd` to monitor the following events:

- File access
- System calls
- Login and logout activity of users

Audit logging enables you to discover access violations, changed or deleted files, failed authentication, and so on.

Viewing audit events in the UI

With the Administrator, Backup Administrator, Restore Administrator, and User roles, you can view audit events to monitor system activity.

About this task

The following actions generate an audit event:

- User login and logout
- Creating, deleting, or updating a user
- Assigning or unassigning a role to a user

To view audit events in the UI, perform the following steps.


Steps


1. Log in to the PowerProtect Data Manager UI with an account that has one of the indicated roles.
2. Go to **Alerts > Audit Logs**.

View and manage 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. With the Administrator, Backup Administrator, Restore Administrator, or User role, you can access the alerts from the **Alerts** window. However, only some of these roles can manage alerts.

Steps

1. From 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.
The **System** tab displays all alert types.
3. To view more details about a specific entry, click  next to the entry in the table.
4. For the following steps, log in to the PowerProtect Data Manager UI with an account that has the Administrator, Backup Administrator, or Restore Administrator role.
5. To acknowledge the alert, select the alerts and then click **Acknowledge**.
6. To add or edit a note for the alert, click **Add/Edit Note**, and when finished, click **Save**.
7. To export a report of alert information to a .CSV file which you can download for Excel, select an entry in the table and then click **Export**.

 **NOTE:** If you apply any filters in the table, exported alerts include only those alerts that satisfy the filter conditions.

Export audit logs

With the Administrator or Security Administrator role, you can export audit log records to a CSV file of audit data that you can download and open in Excel. Only the Administrator role can change the retention period.

Steps

1. Go to **Administration > Audit Logs**.
The list of audit logs appears, which displays the following information:
 - Changed at
 - Audit Type
 - Description
 - Changed By
 - Object Changed
 - Previous Values

- New Values
2. To set the retention period (in days) for the audit log, select **Set Boundaries** and update the retention period. Only the Administrator role can perform this step.
 3. To add a note for the audit log, click **>**, enter a note in the **Note** field, and click **Save**.
 4. Click **Export**.

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 , select **Support**, and then click **System Health**.

The following table provides a summary of each component state:

Table 40. 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.
No response	This state appears when the service that is associated with the component is running, but the service is not responding.

Access the open source software package information

All open source software (OSS) package information used by PowerProtect Data Manager is stored in a common directory.

To access this information, SSH login to PowerProtect Data Manager and retrieve the OSS reports from the `/usr/local/brs/puppet/licenses` directory.

Security certificates

A default installation of PowerProtect Data Manager creates self-signed security certificates that secure communication with other components. As you configure the server and add assets, PowerProtect Data Manager stores additional certificates for each component.

The Administrator and Security Administrator roles can review the **Administration > Certificates** page in the UI. This page contains three tabs that list the installed security certificates. Each tab provides information about certificate uses, expiry dates, issuers, and so forth.

The certificates on the **Internal** tab secure access to components that are part of the PowerProtect Data Manager server, such as the UI and REST API. The certificates on the **Application Agents** tab secure access to the agents, which are under the control of PowerProtect Data Manager but exist outside the server. The certificates on the **External Servers** tab secure access to components or systems that are beyond the control of the server, but where you have approved the communication.

The *PowerProtect Data Manager Security Configuration Guide* contains more information about cryptography and security certificates. This guide provides instructions for how to manage the installed certificates, including important prerequisites, operational considerations, associated tasks, and troubleshooting. For example, you can replace the default self-signed security certificates for with certificates from an approved certificate authority. This guide also contains instructions for establishing certificate-based trust with external components and systems.

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 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.

Steps

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 8. Editing the GNU 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:
 - i. Type **select /dev/sdb**.
 - ii. 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.
 - iii. 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**

- iv. 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.

Steps

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**.

Memory optimization

You can use adjust the amount of memory that is assigned to the PowerProtect Data Manager virtual machine in order to optimize server performance.


The following table indicates the minimum amount of memory to assign to the PowerProtect Data Manager virtual machine in a standard environment.

Table 41. Minimum memory requirements

Deployment Type	Memory
Default	20 GB
With the Cloud Disaster Recovery (Cloud DR) Add-On	24 GB

Consider the following:

- Depending on the environment, increasing the amount of memory can increase performance.
- If low-memory alerts are seen, increase the amount of memory.
- Do not increase the amount of memory beyond 32 GB of RAM. PowerProtect Data Manager is not designed to support more than 32 GB of RAM.
- If you are deploying PowerProtect Data Manager to a virtual machine in a cloud Marketplace environment, it is automatically assigned 32 GB of RAM. This amount of memory should not be changed after it is deployed.

 **NOTE:** For help with optimizing memory, contact your Customer Support representative.

Memory and updating from an earlier version of PowerProtect Data Manager

Features in the current version of PowerProtect Data Manager might require more memory than required in previous versions. When updating from an earlier version of PowerProtect Data Manager, ensure that you increase the amount of assigned memory as necessary.

Adjust the memory

Adjust the amount of memory assigned to the PowerProtect Data Manager to support changes in the protection environment.

Steps

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 32 GB of memory and that it is a multiple of 4 GB.
4. Click **OK**.

Configure the DD system

Prerequisites

Before you can use DD to protect the system, use NFS to export the MTree that PowerProtect Data Manager uses on the DD system. The setup on the DD system requires that you add the PowerProtect Data Manager client with no_root_squash.

Steps

1. Use a web browser to log in to the **DD 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 DD MTree.
 - b. If you have not yet created the DD MTree, follow the prompts to create the MTree and click **Close**.
 - c. In the **Directory path** field, specify the full directory path for DD 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**.

Virtual networks (VLANs)

PowerProtect Data Manager can separate management and backup traffic onto different virtual networks (VLANs). Virtual networks help to improve data traffic routing, security, and organization.

The default configuration routes the management traffic over the same network as backup traffic. All assets are part of the same network.

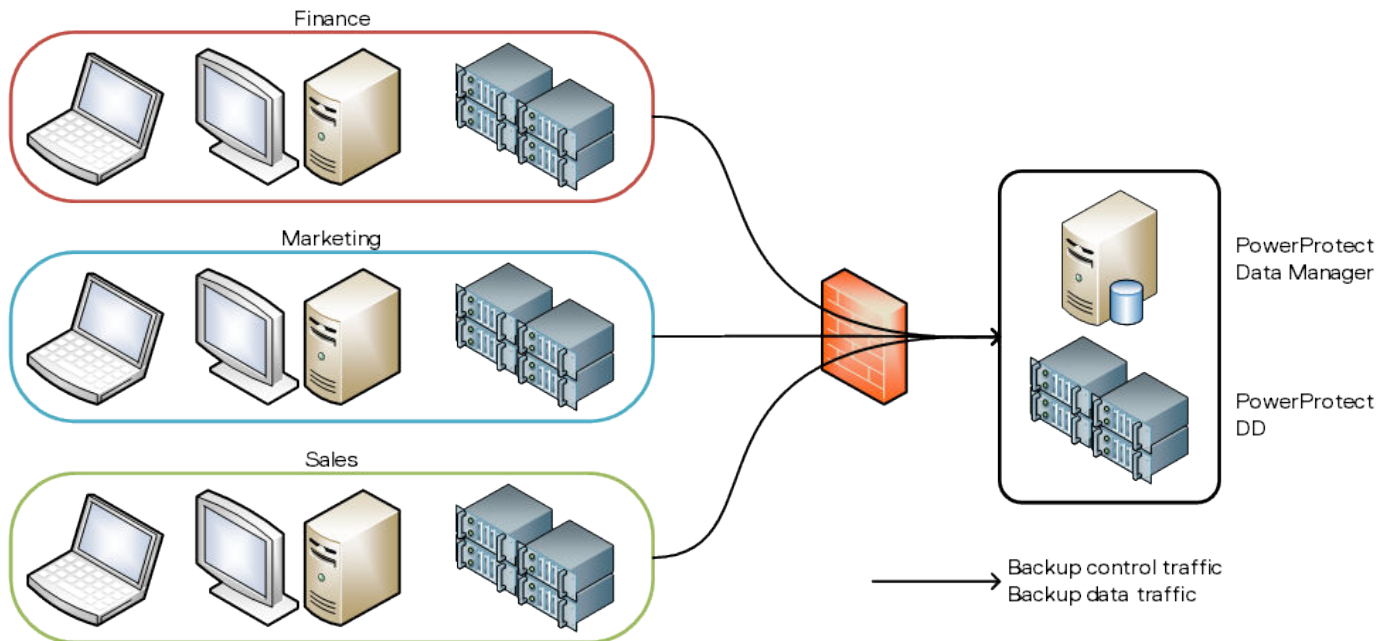


Figure 9. Flat network

You can also configure virtual networks to separate management traffic from backup traffic. This configuration can also separate traffic that originates from different networks. In that case, you can use the same virtual network for management and backup traffic, or separate virtual networks for each.

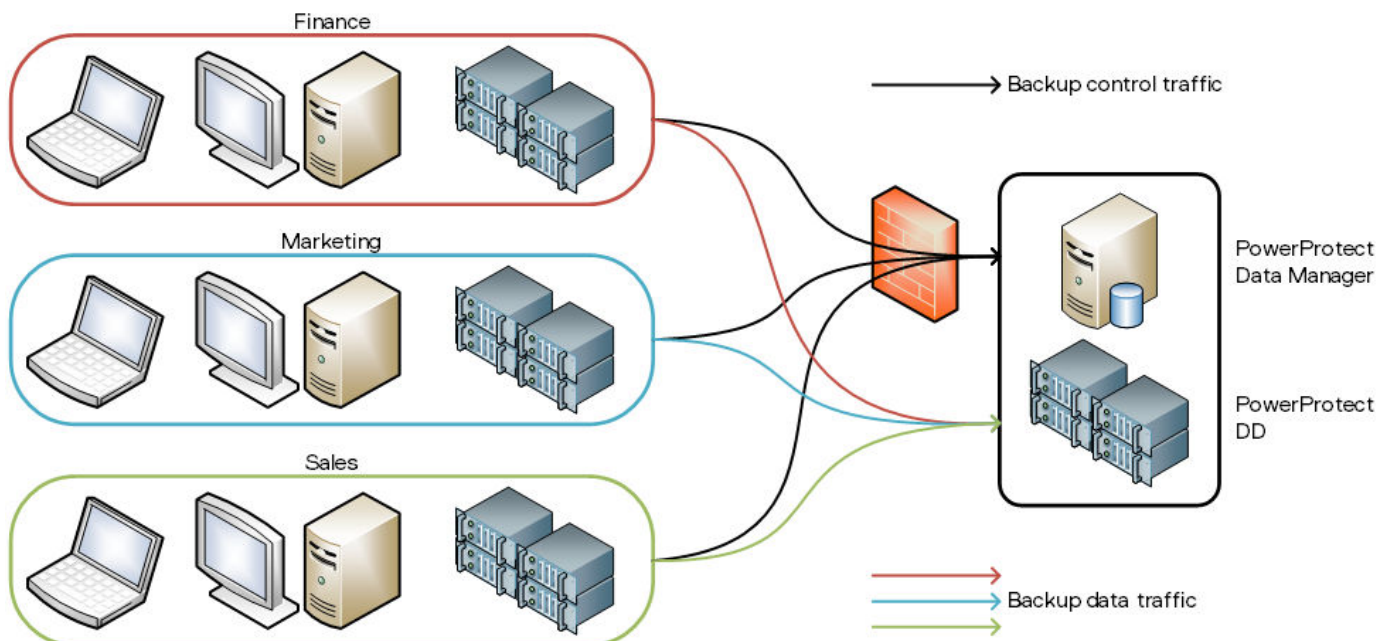


Figure 10. Virtual networks

To use virtual networks with PowerProtect Data Manager, you must configure the DD and network infrastructure before you configure the PowerProtect Data Manager or assign networks to assets.

Configuration follows a multistep workflow:

1. Configure the virtual network on the DD.
2. Add the DD as storage and name the network interface.
3. Add the virtual network to the PowerProtect Data Manager.
4. Register the assets with the PowerProtect Data Manager.
5. Create a protection policy (or edit an existing policy) and assign the preferred virtual network.
6. Optionally, assign the virtual network to individual assets. This action overrides any preferred virtual network that you may have specified through a protection policy.

The initial steps to configure and add each virtual network are one-time events. The subsequent steps to assign virtual networks to protection policies or assets happen as required.

Configuration is nondisruptive. You can add, edit, or delete virtual networks without affecting background activities, disconnecting network interfaces, or affecting the PowerProtect Data Manager user interface.

PowerProtect Data Manager logs network changes in the audit log. Failed network changes appear in the **System** alerts.

Supported scenarios

PowerProtect Data Manager supports virtual networks for the following use cases:

- Virtual machine backups
- Database backups
- Exchange backups
- File system backups
- Replication
- Disaster recovery
- Cloud DR
- Storage Data Management
- Search Engine

NOTE: The first time that you use the **Networks** page to add a virtual network to an environment with existing search engine nodes, PowerProtect Data Manager does not automatically add the virtual network to the search engine. Instead, manually edit each node to add the virtual network. This action makes the search engine aware of virtual networks. Any subsequent new virtual networks are automatically added to the search engine.

Virtual network prerequisites

Before you configure a virtual network, complete the following actions:

- Register the vCenter server on which PowerProtect Data Manager is deployed. You can verify this on the **vCenter** tab of the **Asset Sources** page.
- Configure the network switch port for trunk mode. This setting allows the port to carry traffic for multiple VLANs.
- Enable Virtual Guest Tagging (VGT) mode on the VMware ESXi virtual network switch port for PowerProtect Data Manager.

You can use a standard port group or a distributed port group. For standard port groups, configure the virtual switch port for VLAN ID 4095, which makes all VLANs accessible. Alternatively, you can use VLAN trunking, which supports specifying multiple VLANs by ID or range. The VMware ESXi documentation provides more information.

- Configure a VLAN interface for the DD through the **Interfaces** tab on the **Hardware > Ethernet** window in the DD System Manager. The DD documentation provides more information.

Dell Technologies recommends that you choose an interface name that incorporates the VLAN ID. For example, the interface name `ethv1.850` for VLAN ID 850.

- Add the DD as protection storage for PowerProtect Data Manager.

PowerProtect Data Manager does not verify the network switch configurations. If the physical or virtual network switch is incorrectly configured, then virtual network configuration fails.

Configuring virtual networks

The following topics create and maintain virtual networks in PowerProtect Data Manager for use with assets on different VLANs.

PowerProtect Data Manager names each virtual network in two places: the interface to the protection storage system and the interface to the protected assets. These names are not required to match. However, Dell Technologies strongly recommends that you use the same network name in both locations for each virtual network. Record each network name for later use.

Dell Technologies also recommends that you choose network names that incorporate the VLAN ID. For example, `sales-vlan850` for VLAN ID 850.

Adding a virtual network includes creating a pool of static IP addresses. PowerProtect Data Manager uses these addresses for the local interfaces to the virtual network and for any VM Direct protection engines or search engine nodes that you deploy on this network.

Each VM Direct protection engine or search engine node requires an IP address on the virtual network. The PowerProtect Data Manager interface requires one IP address. Ensure that you have enough IP addresses available on each network to meet this requirement. To prepare for future expansion, you can add more IP addresses than are initially required.

Name the virtual network for protection storage

After you add protection storage, name the virtual network between the PowerProtect Data Manager and the protection storage system. To rename a virtual network (edit the network name), repeat these steps.

Steps

1. From the PowerProtect Data Manager UI, select **Infrastructure > Storage**.
The **Storage** window appears.
2. On the **Protection Storage** tab, select the storage system, and then select **More Actions > Name Network**.
The **Name Network** window opens and displays a list of known network interfaces, assigned IP addresses, and link speeds.
3. Identify the interfaces for each new virtual network, and then type names for the virtual networks in the corresponding fields.
4. Click **Save**.
The PowerProtect Data Manager stores the network names.

Add a virtual network

Configure a new virtual network for use with assets and protection policies.

About this task

Each new virtual network requires at least one IP address for a PowerProtect Data Manager network interface. Review the **Number of IP addresses needed** field before you supply the required static IP addresses.

Steps

1. From the PowerProtect Data Manager UI, select **Infrastructure > Networks**.
The **Networks** window appears.
2. Click **Add**.
The **Add Network** wizard opens.
3. In the **Network Name** field, type the name of the new virtual network.
Dell Technologies recommends that you keep the network names consistent for each VLAN.
4. In the **VLAN ID** field, type the numeric value 1 through 4094 that corresponds to the VLAN which this virtual network represents.
5. Provide the applicable **Subnet Mask** and **MTU** (maximum transmission unit) values for the virtual network.
Allowable **MTU** values range from 1500 to 9000.
6. For the **Static IP Pools** field, provide the indicated number of reserved IP addresses for PowerProtect Data Manager to use for communication on this virtual network.

To add values to the pool, type an IP address or range, and then click **Save**. To remove values from the pool, select a value from the pool, and then click **Delete**.

You can type each IP address separately, or you can provide an IP address range in the form **10.1.1.4–10.1.1.10**.

7. Verify that the static IP address pool contains enough addresses to add the virtual network.
8. Click **Next**.
The **Add Network** wizard moves to the **Routes** page.
9. If applicable, click **Add** to define any required routes.
The **Add Routes** page opens. Complete the following substeps:
 - a. Select a route type:
 - If you select **Subnet**, define the subnet in CIDR format. For example, 10.0.0.0/24.
 - If you select **Host**, type the IP address.
 - b. Type the IP address of the default gateway through which PowerProtect Data Manager should reach the subnet or host.
 - c. Click **Add**.
The **Add Routes** page closes. The **Routes** list displays the new route.
 - d. Review the route information.
If any parameters are incorrect, select the checkbox for that route and then click **Delete**.
 - e. Repeat these substeps for any additional required routes.
10. Click **Next**.
The **Add Network** wizard moves to the **Summary** page.
11. Verify the network configuration information, and then click **Finish**.
The **Add Network** wizard closes. The **Networks** page displays the new network with the *Initiating* status.

Next steps

PowerProtect Data Manager may take a short time to configure the virtual network.

If the virtual network status changes to *Failed*, then a corresponding system alert contains more information about the cause of the failure. Troubleshoot the failure and then complete one of the following actions:

- If the failure was caused by a configuration issue, click **Edit** to update the network configuration.
- If the failure was transient or had an external cause, and the configuration is correct, click **Retry** to use the same settings.

NOTE:


When you edit or retry a virtual network operation that failed and there are additional IP addresses in the address pool, PowerProtect Data Manager marks the last failed IP address as abandoned. PowerProtect Data Manager does not try to reuse any IP addresses that are marked as abandoned. The UI does not display this condition.

[KB article 000181120](#) provides more information about how to use the REST API to detect when an IP address is marked as abandoned. The article also provides steps to correct this condition so that the IP address can be used again.

View the details of a virtual network

If the virtual network name is ambiguous or does not contain the VLAN ID, you can view the details to further identify the virtual network before making changes.

Steps

1. From the PowerProtect Data Manager UI, select **Infrastructure > Networks**.
The **Networks** window appears.
2. Locate the row that corresponds to the appropriate virtual network.
The columns for each row indicate the associated VLAN ID and network status.
3. Click  for that row.
The **Details** pane opens to the right.
This pane contains information about the virtual network configuration, such as the assigned IP address for the PowerProtect Data Manager backup interface to that network, and any configured routes.
4. Click **X** to close the details pane.

Edit a virtual network

You can change any parameter for a virtual network without deleting the network. For example, to add more IP addresses to the static IP pool.

Prerequisites

If an IP address from the static IP pool is already in use, you cannot remove the address from the pool.

Steps

1. From the PowerProtect Data Manager UI, select **Infrastructure > Networks**.
The **Networks** window appears.
2. Locate the row that corresponds to the appropriate virtual network, and then click the radio button to select that row.
The PowerProtect Data Manager enables the **Edit** and **Delete** buttons.
3. Click **Edit**.
The **Edit Network** wizard opens to the **Summary** page.
4. Click **Edit** for the **Configuration** or **Routes** sections.
The **Edit Network** wizard moves to the **Configuration** or **Routes** page.
5. Modify the appropriate network parameters, and then click **Next**.
The **Edit Network** wizard moves to the **Summary** page.
6. Verify the network configuration information, and then click **Finish**.
The **Edit Network** wizard closes. The **Networks** page reflects the updated information, where applicable.
You may need to view the details for the virtual network to verify some changes.

Delete a virtual network

Although optional, Dell Technologies recommends that you delete virtual networks when they are no longer required.

Prerequisites

Unassign the virtual network from any applicable assets. Disable all VM Direct Engines that are configured to use the virtual network. Disable any search cluster that uses the virtual network.

Steps

1. From the PowerProtect Data Manager UI, select **Infrastructure > Networks**.
The **Networks** window appears.
2. Locate the row that corresponds to the appropriate virtual network, and then click the radio button to select that row.
PowerProtect Data Manager enables the **Edit** and **Delete** buttons.
3. Click **Delete**.
4. Verify the network information, and then click **OK** to acknowledge the deletion warning.
The PowerProtect Data Manager removes the virtual network from the list on the **Networks** page.

Virtual network asset assignment

Assignments identify which assets should use each virtual network. There are two methods to associate an asset with a virtual network:

- By protection policy

You can configure the PowerProtect Data Manager to choose a preferred virtual network for all assets on a protection policy.

- By asset

You can assign virtual networks to individual assets. This method is optional and overrides any virtual network assignment from a protection policy. Assets which are not individually assigned automatically use the preferred virtual network.

You can use this method to specify a virtual network for any asset. However, this method is especially suited to configuring assets which are exceptions to the rule. You can also split assets on the same application host across multiple virtual networks. For example, when an asset has its own network interface or belongs to another department.

Dell Technologies recommends that you assign assets to virtual networks by protection policy, where possible.

Before you assign an asset, perform the following actions:

- Test connectivity from the asset host to the PowerProtect Data Manager by pinging the PowerProtect Data Manager IP address on that virtual network.
- Register the asset source with the PowerProtect Data Manager.
- Approve the asset source.

Assign a virtual network by protection policy

The following steps apply a virtual network to an existing protection policy. You can also assign a virtual network when you create a protection policy.

About this task

The **Network Interface** field selects the network interface for communication with the destination protection storage system. This network carries the backup data.

Steps

1. From the PowerProtect Data Manager UI, select **Protection > Protection Policies**. The **Protection Policies** window appears.
2. Locate an existing protection policy for which you want to configure a virtual network.
3. Select the radio button for the protection policy, and then click **Edit**. The **Edit Policy** wizard opens to the **Summary** page.
4. In the **Objectives** block, click **Edit**. The **Edit Policy** wizard moves to the **Objectives** page.
5. Select the checkbox for the appropriate schedule.
6. In the **Network Interface** field, select the correct virtual network from the list.

Each list entry indicates the interface name, interface speed, and virtual network name.

If the network was not named, a combination of the interface name and VLAN ID replaces the virtual network name. For example, `ethV1.850`. An interface without a virtual network name behaves as if a virtual network was not configured.


7. Click **Next**. The **Edit Policy** wizard moves to the **Summary** page.
8. Verify the policy information, and then click **Finish**. Ensure that the selected assets are part of the virtual network. The **Edit Policy** wizard closes.
9. Click **OK** to acknowledge the update, or click **Go to Jobs** to monitor the update.

Assign a virtual network by asset

This procedure is optional. You can assign a virtual network for individual assets or for all assets on a particular application host.

About this task

This setting overrides the network assignment from the protection policy. If PowerProtect Data Manager cannot use this network assignment for any reason, the setting falls back to the assignment from the protection policy.

 **NOTE:** You cannot back up individual assets across different networks on the same protection policy and application host. Instead, create a separate protection policy for the assets on each network.

Steps

1. From the PowerProtect Data Manager UI, select **Infrastructure > Assets**.

The **Assets** window appears.

2. Locate the appropriate assets from the list on any tab.
Use the checkbox to select each asset. You can select more than one asset at a time.
3. Click **More Actions > Assign Network**.
The **Associated Assets** window opens.
4. To use the virtual network for all assets on the same application host, click **Include**.
Otherwise, to use the virtual network for only the selected assets, click **Do Not Include**. Consider whether you require a separate protection policy for assets on different networks.
The **Assign Network** window opens.
5. Select a virtual network from the **Network Label** list, and then click **Save**.

Results

The PowerProtect Data Manager applies the network selection to the selected assets. The **Network** column in the list of assets for each tab now indicates the selected virtual network.

Protecting Virtual Machines using the Transparent Snapshot Data Mover

Topics:

- Overview of transparent snapshots for virtual machine protection
- VIB installation monitoring and management
- Transparent snapshot data mover system requirements
- Prerequisites to virtual machine protection with the Transparent Snapshot Data Mover
- Virtual machine transparent snapshot unsupported features and limitations
- Transparent Snapshot Performance and Scalability

Overview of transparent snapshots for virtual machine protection

The transparent snapshot data mover (TSDM) is a new protection mechanism in PowerProtect Data Manager 19.9 and later designed to replace the VMware vStorage API for Data Protection (VADP) protection mechanism for crash-consistent virtual machine protection.

The advantages of using the TSDM protection mechanism for virtual machine data protection include the following:

- Eliminates the latency and performance impact on the production virtual machine during the protection policy life cycle.
- Reduces the CPU, storage, and memory consumption required for backups. After the initial full backup, only incremental backups using the immediate previous snapshot will be performed.
- An external VM Direct engine is not required. The VM Direct engine embedded with PowerProtect Data Manager is sufficient.
- Automatic scaling.

VIB installation monitoring and management

The vSphere Installation Bundle (VIB) is a software package that is bundled with the PowerProtect Data Manager OVA and update package and is installed automatically on a vSphere ESXi host during the PowerProtect Data Manager 19.9 installation or update. The VIB is required to enable the transparent snapshot data mover (TSDM) for virtual machines.

An entry for the job **Performing Host Configuration (vib_install)** appears in the PowerProtect Data Manager UI during the VIB installation. During the installation, vCenter and ESXi host information is detected to verify the supported versions are installed.

You can use the **Transparent Snapshot Data Movers** tab in the **Protection Engines** window of the PowerProtect Data Manager UI to monitor and manage the installation of the VIB. This window provides a vCenter hierarchy view based on the asset sources enabled in PowerProtect Data Manager. If an ESXi host is not eligible or available for the VIB installation, the status displays as **Not Eligible** in the **Protection Engines** window.

During the creation of a crash-consistent virtual machine protection policy, the VIB is deployed automatically on the vSphere cluster being protected. If all requirements are met, TSDM is used as the default protection mechanism instead of VADP. Existing policies created in PowerProtect Data Manager 19.8 and earlier can be migrated to use TSDM, provided that the virtual machine crash-consistent policies are configured with the following options:

- **Performance** optimization mode.
- **Exclude swap files from backup** is off.
- **Enable guest file system quiescing** is off.

You can use the PowerProtect Data Manager UI to apply TSDM as the data mover for virtual machine assets.

Transparent snapshot data mover system requirements

The following software is required to automatically enable use of the Transparent Snapshot Data Mover (TSDM) for virtual machine data protection operations.

NOTE: TSDM for virtual machine protection also requires that the protection policy is a performance optimized crash-consistent policy, with the quiescing and swap file exclusion options disabled.

Table 42. Software requirements

Software required	Version supported	Notes
vCenter Server	7.0 U3	vCenter and ESXi 7.0 U3 is the minimum version that is required to use TSDM, and is scheduled for release shortly after the availability of PowerProtect Data Manager 19.9. Until this version is available and installed in the environment, TSDM is not used for virtual machine protection policies.
ESXi Server	7.0 U3	
PowerProtect Data Manager software	19.9 and later	

Prerequisites to virtual machine protection with the Transparent Snapshot Data Mover

Review the following recommendations for use of the Transparent Snapshot Data Mover (TSDM) protection mechanism for virtual machine protection.

Additional privileges required for a dedicated vCenter user account to use Transparent Snapshot Data Mover

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 additional privileges required to use the Transparent Snapshot Data Mover (TSDM) for virtual machine protection operations.

NOTE: For the remaining privileges required for the dedicated vCenter user account, see [Specify the required privileges for a dedicated vCenter user account](#) on page 64.

Table 43. Minimum required vCenter user account privileges

Setting	vCenter 7.0.3 and later required privileges	PowerCLI equivalent required privileges
Datastore	<ul style="list-style-type: none">• Datastore > File Management	<pre>\$privileges = @('Host.Config.Patch', 'Host.Config.Image', 'Host.Config.NetService', 'Datastore.FileManagement', 'vSphereDataProtection.Protection', 'vSphereDataProtection.Recovery', 'System.Read')</pre>
Host	<ul style="list-style-type: none">• Configuration > Patch• Configuration > Image• Configuration > Net Service• Datastore > File Management	
System	<ul style="list-style-type: none">• System > Read	
vSphere Data Protection	<ul style="list-style-type: none">• Protection• Recovery	

Table 43. Minimum required vCenter user account privileges (continued)

Setting	vCenter 7.0.3 and later required privileges	PowerCLI equivalent required privileges
		<code>New-VIRole -Name 'PowerProtect' -Privilege (Get-VIPrivilege -Id \$privileges)</code>

Creating VMkernel ports

For backup and restore of virtual assets from the ESXi hosts and their respective virtual machines using the Transparent Snapshot Data Mover (TSDM) protection engine, Dell Technologies strongly recommends that you create a dedicated VMkernel port for all ESXi hosts in the cluster to facilitate data transfer.

Before you begin

- For optimal data transfer between ESXi hosts and protection storage, use the same network subnet that is used for backup storage.
- For each ESXi host in the cluster, it is recommended to use a 10G physical network adapter port for TSDM backup traffic.
- Plan a unique network subnet to use exclusively for TSDM protection engine that does not overlap with any other existing network subnets. This subnet must contain the following:
 - An IP address for each VMkernel port in each ESXi host.
 - An IP address for each port in protection storage target interfaces.

Create a VMkernel port for a standard vSwitch configuration

For each ESXi host in the cluster:

1. In the **vSphere Client**, navigate to the ESXi host and select the host.
2. Right-click the host and select **Add Networking**.
3. Select **VMkernel Network Adapter**, and then click **Next**.
4. Create a new switch, or choose an existing one, following the recommendations above. When creating a new switch, assign the NIC adapter to **Active Adapters**.
5. In the **Port Properties** settings **IP settings**, select **IPv4**, and clear all other check boxes under **Available services**.
6. In the IPv4 settings, specify VMkernel IPv4 settings following the recommendations above.

Create a VMkernel port for a Distributed vSwitch configuration

1. On the **vSphere Client** home page, click **Networking**, and then navigate to and select a distributed port group.
2. From the **Actions** menu, select **Add VMkernel Adapters**.
3. On the **Select hosts** page, click **Attached hosts**, select from the hosts that are associated with the distributed switch, and then click **OK**.
4. Click **Next**.
5. On the **Configure VMkernel adapter** page, select **IPv4**, and clear all other check boxes under **Available services**.
6. In the IPv4 settings, specify VMkernel IPv4 settings following the recommendations above.

Virtual machine transparent snapshot unsupported features and limitations

Review the following unsupported features and limitations for the transparent snapshot data mover (TSDM) in PowerProtect Data Manager 19.9.

Unsupported virtual machine configurations

The following virtual machines and configurations are not supported for TSDM virtual machine protection:

- vVOL Datastores
- Physical RDMs
- Virtual RDMs
- Encrypted virtual machines
- Fault Tolerant virtual machines.

Virtual Machine Disk (VMDK) limit for virtual machines protected with TSDM

TSDM-based protection supports a maximum of 40 VMDKs per virtual machine. If this limit is exceeded, backups will be queued for a longer period of time, and will have to be cancelled manually.

For virtual machines with more than 40 VMDKs, you can override the protection mechanism at the asset level to use VADP. The section [Migrating assets to use the Transparent Snapshot Data Mover](#) on page 71 provides more information.

vMotion of TSDM protected virtual machines

vSphere disables the vMotion migration of virtual machines to an ESXi host version previous to 7.0 U3 when the virtual machine is protected with TSDM. In order to migrate the TSDM protected virtual machine to an ESXi version that does not support TSDM, you must disable the Lightweight Delta (LWD) filter that is attached to the virtual machine during the initial protection policy configuration. To disable the filter, remove the virtual machine from the TSDM protected virtual machine protection policy. Once the virtual machine is removed from the policy, a job is automatically initiated to disable the filter.

Once the vMotion completes, you can re-add the virtual machine to the protection policy. This virtual machine will then be protected by the VADP protection mechanism, since the new ESXi/cluster host version is lower than the version required by TSDM.

Removal of managed snapshots required prior to running virtual machine protection policies

A PowerProtect Data Manager virtual machine protection policy cannot be configured to use the TSDM protection mechanism when the virtual machine contains managed snapshots. Verify that no managed snapshots exist for the virtual machine, and then retry the configuration job from the **System Jobs** window of the PowerProtect Data Manager UI.

TSDM only available for virtual machine crash-consistent policies

Use of the TSDM protection mechanism is currently only supported for crash-consistent virtual machine protection policies. Also, the virtual machine crash-consistent policy must use the **Performance** optimization mode, with swap file exclusion and quiescing turned off.

Cloud Disaster Recovery not supported

Cloud Disaster Recovery (CDR) is not supported for TSDM virtual machine backups up PowerProtect Data Manager 19.9.

Transparent Snapshot Performance and Scalability

Review the following information related to performance considerations to scale your environment.

NOTE: As a VMware infrastructure best practice, Dell Technologies recommends spreading the workload across ESXi Servers as much as possible. With the Transparent Snapshot Data Mover protection mechanism, you can move backup data in streams from multiple ESXi Servers.

Table 44. Scalability limits for the vCenter and ESXi Server

Component	Maximum limit
Number of protected virtual machines per ESXi Server	Unlimited
Number of VMDKs that can be protected per ESXi Server	1000
Size of VMDK	64 TB
Transparent Snapshot Data Mover (TSDM)	Up to 3000 virtual machine backups, and up to 180 concurrent virtual machine backups. NOTE: An external VM Direct engine is not required when using TSDM as the protection mechanism for crash-consistent virtual machine protection. For application consistent and application aware virtual machine protection, add an external VM Direct engine.

PowerProtect Functionality Within the vSphere Client

Topics:

- [PowerProtect functionality within the vSphere Client](#)
- [Overview of the PowerProtect plug-in for the vSphere Client](#)
- [Overview of VASA and VMware Storage Policy Based Management](#)

PowerProtect functionality within the vSphere Client

The **vSphere Client** integrates with PowerProtect Data Manager to provide the following functionality:

- **PowerProtect** portlet—When adding a vCenter Server as an asset source in the PowerProtect Data Manager UI, if you enable the **vSphere Plugin** option, a pane for **PowerProtect** appears in the **vSphere Client**. This pane provides a subset of PowerProtect Data Manager functionality, including the availability to perform a manual backup, image-level restore and file-level restore of PowerProtect Data Manager virtual machine protection policies.
- Storage policy association with a PowerProtect Data Manager virtual machine protection policy—vSphere Storage APIs for Storage Awareness (VASA) leverages VMware Storage Policy Based Management (SPBM) to support data protection operations, allowing you to pair SPBM policies that are created in the **vSphere Client** with protection policies that are created in PowerProtect Data Manager. This association allows you to manage all virtual machine storage and protection requirements in a centralized location (the **vSphere Client**), instead of requiring multiple user interfaces.

Overview of the PowerProtect plug-in for the vSphere Client

When adding a vCenter Server in the PowerProtect Data Manager UI, if you enable the **vSphere Plugin** option, a subset of the UI functionality becomes available within the **vSphere Client**.

The PowerProtect Data Manager portlet appears when you select **Hosts and Clusters** or **VMs and Templates** in the left pane of the **vSphere Client** home page, and then select a virtual machine within the datacenter.

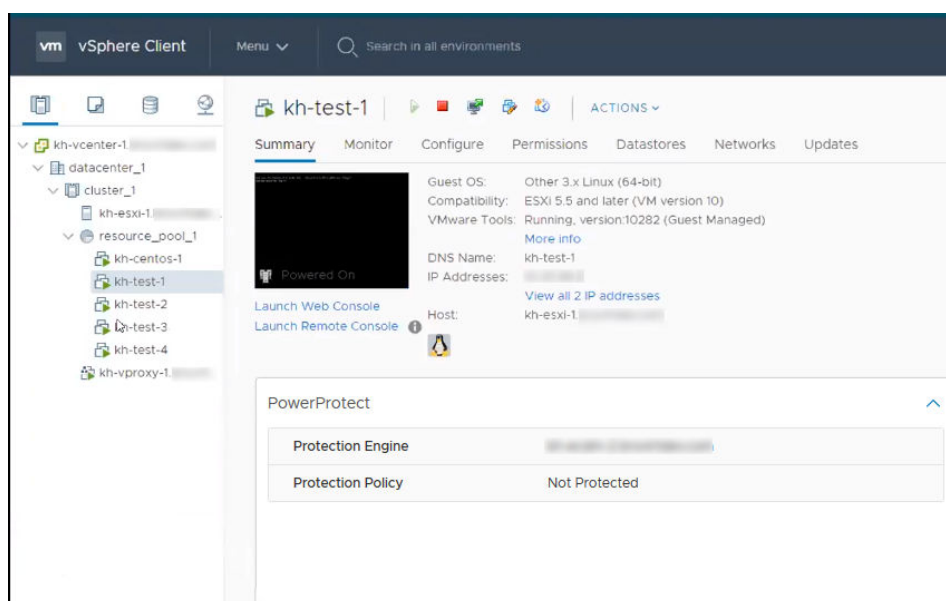


Figure 11. PowerProtect portlet in the vSphere Client

NOTE: If you were already logged into the **vSphere Client** when the vCenter discovery was started in PowerProtect Data Manager, you must log out and log back in to see the PowerProtect Data Manager UI.

If the virtual assets in the vCenter have not yet been assigned to a PowerProtect Data Manager protection policy, only the **PowerProtect** name displays in the portlet. Adding the virtual machine to a protection policy provides additional information, as shown in the following figure.

PowerProtect	
Protection Engine	kh-ecdm-2. .com
Protection Policy	test
Last Protection Copy	Aug 16, 2019, 10:01:56 AM
Consistency	Crash Consistent
Size	715.0 MiB
Retention	Aug 22, 2019, 5:00:00 PM

Figure 12. PowerProtect portlet with protected virtual machine

After you set up a virtual machine protection policy, you can perform the following PowerProtect Data Manager functionality within the **vSphere Client**:

- View information about protection policies and information about available protection copies.
- Monitor in-progress backup and restore operations for the virtual machine protection policy. You can also view information for successfully completed protection copies that are available for restore.
- Perform a manual backup.
- Perform an image-level restore (Restore to Original, Restore to New, or Instant Access).
- Perform a file-level restore.

Prerequisites for enabling the vSphere Client PowerProtect plug-in

To use the **vSphere Client PowerProtect** plug-in for backup and restore operations, complete the following tasks in the **vSphere Client** and the PowerProtect Data Manager UI.

- Add the vCenter Server—In the PowerProtect Data Manager UI, select **Infrastructure > Asset Sources**, and move the **vSphere Plugin** slider to the right to enable the plug-in. [Add a VMware vCenter Server](#) on page 62 provides information.

- Add privileges for the **Virtual machine power user** group (if you are already an administrator, this task is optional)—In the **vSphere Client**, go to **Administration > Roles**, select the **Virtual Machine power user (PPDM)**, and then open the **Edit Role** window.

Add the following PowerProtect Data Manager privileges:

- Backup
- File Level Restore to Original
- Instant Access
- Restore to New
- Restore to Original

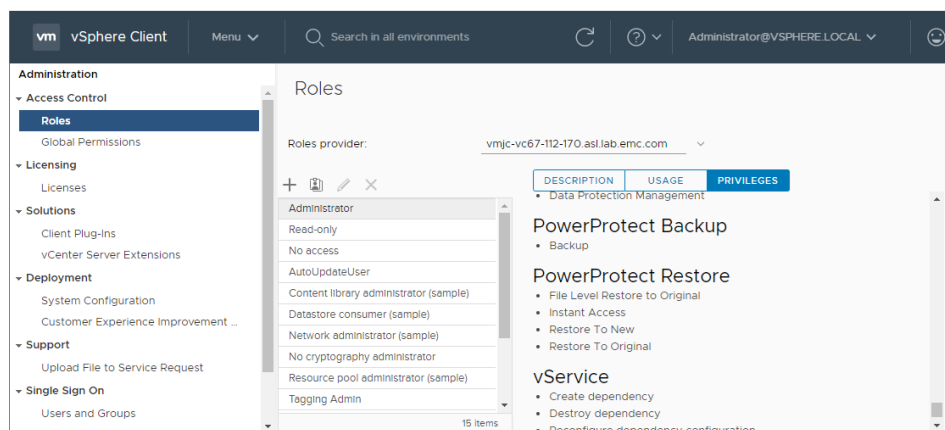


Figure 13. PowerProtect privileges added for the Virtual machine power user

- 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 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 **Protection > Protection Policies** window to schedule a backup of the virtual machines. [Add a protection policy for virtual-machine protection](#) on page 77 provides information.

Monitor PowerProtect Data Manager virtual machine protection copies

You can use the **Monitor** tab in the **vSphere Client** to view PowerProtect Data Manager protection copies that are available for restore, and monitor in-progress backup and restore operations for the PowerProtect Data Manager virtual machine protection policy.

With a virtual machine selected, in the **Monitor** tab's navigation pane, select **PowerProtect > Protection Copies** to view information about completed PowerProtect Data Manager protection policy backups for this virtual machine. This view is the same as the view in the PowerProtect Data Manager UI **Infrastructure** window. A copy map enables you to view the available protection copies when you click on the storage icon, as described in [More options for managing virtual-machine backups](#) on page 85.

To view the status of active backup and restore operations initiated from the PowerProtect Data Manager UI or the **vSphere Client**, click the arrows icon in the lower right corner of the window to expand the **Recent Tasks** pane. You can also view this pane from the **Summary** window.

Manual PowerProtect policy backup in the vSphere Client

You can back up one or more PowerProtect Data Manager virtual machine protection policies at any time by performing a manual backup in the **vSphere Client**.

Prerequisites

- Ensure that you are logged in to the **vSphere Client** as an administrator.
- Add the **Backup** privilege to the **Administrator** group in the **vSphere Client**. To add the **Backup** privilege, complete the following steps:
 1. Select **Administration > Roles**.
 2. Select **Administrator**, and then click **Privileges** in the right pane.
 3. In the **PowerProtect Backup** section, select **Backup**.
- Ensure that virtual machine assets have been added to a virtual machine protection policy. You cannot perform manual backups of unprotected virtual machines.

Steps

1. In the left pane of the **vSphere Client** home page, select **Hosts and Clusters** or **VMs and Templates**, and then select a virtual machine within the datacenter.
The **Summary** window displays.
2. Perform a manual backup of a virtual machine protection policy by using one of the following methods:
 - In the left pane, right-click the virtual machine, and then select **PowerProtect > Backup**.
 - Within the **PowerProtect** portlet, click **Backup Now**.The **vSphere Client** starts the backup operation. A message appears indicating whether the request was processed successfully.

Results

An entry for the backup job appears in the **Jobs > Protection** window of the PowerProtect Data Manager UI. To view the status of operations, you can also click the arrows icon in the lower right corner of the window to expand the **Recent Tasks** pane.

Image-level restore of a PowerProtect backup in the vSphere Client

You can use the **vSphere Client PowerProtect** plug-in to perform an image-level restore of a PowerProtect Data Manager virtual machine protection policy backup.


About this task

Available image-level restore options in the **vSphere Client** include:


- Restore to Original—Restore the virtual machine to the original location on the same vCenter.
- Restore Individual Virtual Disks—Restore selected VMDKs to the original location on the same vCenter.
- Restore to New—Restore the virtual machine to a new location on the original vCenter.
- Instant Access—Restore the backup as a live virtual machine to 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.


Steps

1. In the left pane of the **vSphere Client** home page, select **Hosts and Clusters** or **VMs and Templates**, and then select a virtual machine within the datacenter.
2. In the **Summary** window, access the backup copy by using one of the following methods:
 - In the left pane, right-click the virtual machine, and then select **PowerProtect > Restore**.
 - Within the **PowerProtect** portlet, click **Restore**.
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. In the **Choose Copy** dialog:
 - a. Select the storage icon to access the backup copies.
 - b. Choose from one of the available copies that appears in the table.
 - c. Click **OK** to close the dialog and return to the **Select Copy** page.
 - d. Click **Next**.
5. On the **Purpose** page, select from one of the following options:
 - Restore Entire VMs—Select this option if you want to restore the entire virtual machine.
 - Restore Individual Virtual Disks—Select this option if you want to restore only specific virtual machine disks (VMDKs).

 **NOTE:** Individual VMDKs can only be restored to the original location.
6. Click **Next**.
If restoring entire virtual machines, the **Restore Type** page appears. If restoring individual VMDKs, the **Select Disks** page appears.
7. On the **Restore Type** page, select from one of the available restore types.
 - For Instant Access restore, review the section [Instant access virtual machine restore](#) on page 117.
 - For Restore to New, review the section [Restore to a new virtual machine](#) on page 115.
 - For Restore to Original, review the section [Restore to the original virtual machine](#) on page 112.
 - For Restore Individual Virtual Disks, review the section [Restore individual virtual disks](#) on page 114.The wizard updates to display the options specific to the restore type that you selected.

 **NOTE:** Options such as vCenter, resource pool, and datastore are limited to the logged-in vSphere user's permissions, and are not necessarily the same as a PowerProtect Data Manager administrator.
8. Click **Next**. The **Summary** page appears.
9. Review your selections and then click **Restore**.

Results

An entry for the restore job appears in the **Recent Tasks** pane of the **vSphere Client** and in the **Restore > Running Sessions** window of the PowerProtect Data Manager UI.

Next steps

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 appears within the **PowerProtect** portlet. If you need extra time for this session, you can click **Extend Session** and increase session availability by up to 7 days.

File-level restore of a PowerProtect backup in the vSphere Client


You can use the **PowerProtect** portlet in the **vSphere Client** to perform a file-level restore of a PowerProtect Data Manager virtual machine protection policy backup.

Prerequisites

Note the following before performing file-level restore in the **vSphere Client**:

- A minimum vCenter version 6.7 U1 is required.
- Review the section [Supported platform versions for file-level restore](#) for supported platform and operating system versions.
- Review the section [File-level restore and SQL restore limitations](#) on page 247.
- Ensure that the **FLR Agent** is installed on the target virtual machine by logging into the virtual machine and verifying that the agent package is installed and the agent process is running. If the **FLR Agent** is not installed, the installation is initiated automatically when you start the mount.

When installing the **FLR Agent** on Windows virtual machines, the user must be an administrator account. When installing the **FLR Agent** on Linux virtual machines, the user must be the root user account. The section [FLR Agent for virtual machine file level restore](#) on page 248 provides more information.

 **NOTE:**
For file-level restores, you can only restore files:

- From a Windows backup to a Windows machine, or from a Linux backup to a Linux machine.
- To virtual machines within the same vCenter.

About this task

Available file-level restore options in the **vSphere Client** include:

- Restore single or multiple files to the original folder and overwrite the original files within the same virtual machine, or
- Restore single or multiple files to a new folder with a new name within the same virtual machine.

Steps

1. In the left pane of the **vSphere Client** home page, select **Hosts and Clusters** or **VMs and Templates**, and then select a virtual machine within the datacenter.
The **Summary** window displays.

2. Access the backup copy by using one of the following methods:
 - In the left pane, right-click the virtual machine, and then select **PowerProtect > File Level Restore**.
 - Within the **PowerProtect** portlet, click **File Level Restore**.

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. In the **Choose Copy** dialog:
 - a. Select the storage icon to access the backup copies.
 - b. Choose from one of the available copies that appears in the table.
 - c. Click **OK** to close the dialog and return to the **Select Copy** page.
 - d. Click **Next**.
5. On the **Mount Copy** page:
 - a. To initiate the disk mount, type the guest operating system user credentials:
 - If there are administrator-level credentials associated with the virtual assets or protection policy being restored, specify end-user credentials.
 - If there are no administrator-level credentials associated with the virtual assets or protection policy being restored, specify administrator credentials. These credentials will be handled as end-user credentials.
 - b. (Optional) Leave **Keep FLR Agent Installed** selected when 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.

If not already installed, the **FLR Agent** is installed on the target virtual machine. A progress bar indicates when the mount completes.

NOTE: You cannot browse the contents of the virtual machine backup until the mounting of the destination virtual machine completes successfully.

- d. Upon successful mount, click **Next**.
6. On the **Select Files to Recover** page:
 - a. Expand individual folders to browse the original virtual machine backup, and select the objects that you want to restore to the destination virtual machine.
 - b. Click **Next**.

NOTE: In the browse view, each directory or hard drive appears twice. Selecting an object from one location selects the object in the duplicate location as well.

7. On the **Options** page, select from one of the following options:
 - Restore to Original Folder and Overwrite Original Files—Select this option to restore all selected files to their original location on the original virtual machine.
 - Restore to an Alternate Folder—Select this option if you want to restore to a new folder in a new location on the original virtual machine.
8. Click **Next**.

If performing the restore to the original virtual machine, the **Summary** page displays. You can go to the final step. If performing the restore to an alternate location on the original virtual machine, the **Restore Location** page displays.

9. On the **Restore Location** page:
 - a. Browse the folder structure of the virtual machine to select the new folder where you want to restore the objects.
 - b. Click **Next**.
10. On the **Summary** page:
 - a. Review the information to ensure that the restore details are correct. You can click **Edit** next to the **Restore Location** or **Files Selected** rows to change the information.
 - b. Click **Restore**.

Results

An entry for the restore job appears in the **Recent Tasks** pane of the **vSphere Client** and in the **Restore > Running Sessions** window of the PowerProtect Data Manager UI.

Overview of VASA and VMware Storage Policy Based Management

vSphere Storage APIs for Storage Awareness (VASA) is a set of application program interfaces (APIs) that allow arrays to integrate with vCenter for management functionality. Storage Vendor Providers allow the vCenter Server to retrieve information from storage arrays, including topology, capabilities (such as native thin provisioning and deduplication), and status. The policy-based management functionality of a VASA provider helps administrators choose the appropriate storage device, and monitors and reports information about existing storage policies.

Starting in vSphere version 7.0 U1, VASA support is extended to Data Protection operations by leveraging VMware Storage Policy Based Management (SPBM). SPBM spans all storage offerings from VMware, allowing policies to provision and manage storage for any virtual machine application. The integration of PowerProtect Data Manager and SPBM allows you to:

- Pair SPBM policies with protection policies, allowing you to meet virtual machine storage and protection requirements within vSphere without requiring the PowerProtect Data Manager UI for data protection operations.
- Add new or existing virtual assets to an SPBM policy. You can also reassign these assets and remove them from the policy.
- View policy compliance status, including data protection policy information.
- Protect virtual machines at scale, allowing you to manage capacity resources and overcome challenges such as capacity planning and different service level requirements.

Enabling VASA and SPBM within the **vSphere Client** for integration with PowerProtect Data Manager requires you to perform the following:

- Register the VASA provider to allow for storage provisioning information flow between PowerProtect Data Manager and the vCenter Server.
- Select the PowerProtect Data Manager storage awareness provider within the vCenter Server storage policy component creation workflow, which exposes the list of available PowerProtect Data Manager virtual machine protection policies.
- Assign the PowerProtect Data Manager protection policy to an SPBM policy, which is automatically assigned to virtual machines when they are represented by an instance.
- Monitor the status of storage compliancy of the virtual assets protected by these PowerProtect Data Manager policies.

If you replace the default self-signed security certificates for PowerProtect Data Manager with certificates from an approved certificate authority, you must exchange the new security certificates with vCenter. The *PowerProtect Data Manager Security Configuration Guide* provides instructions.

Register the VASA provider for policy association

The following procedure describes how to register the VASA provider to enable PowerProtect Data Manager communication with the vCenter Server and use the provider to enable an association between a virtual machine storage policy and a PowerProtect Data Manager virtual machine protection policy.

Prerequisites


The vSphere version must be a minimum 7.0 U1.

Steps

1. In the **vSphere Client**, go to **Menu > Hosts and Clusters**.


2. In the left pane, select the vCenter Server, and then select the **Configure** tab.
3. Under **Security**, select **Storage Providers**, and then click **+ Add**.
The **New Storage Provider** dialog appears.
4. On the **New Storage Provider** dialog:
 - a. Specify a name for the provider.
 - b. Specify a URL in the format **https://my-ppdm.example.com:9009/vasa/version.xml**, where *my-ppdm.example.com* is the PowerProtect Data Manager fully qualified hostname.
 - c. Provide PowerProtect Data Manager credentials for a user with the Administrator role, and then click **OK**.
These credentials are only required for the initial login to perform the registration. Subsequent log-in attempts use certificates.

If the vCenter Server does not trust the SSL certificate of the PowerProtect Data Manager server, a prompt appears, asking if you want to accept the certificate as trusted. You can trust this certificate, or alternatively, you can securely obtain a copy of the certificate as a file, and then click **Browse** within this prompt to select and trust the certificate. The vCenter documentation provides more information.

 **NOTE:** For self-signed or untrusted certificates, an error might appear. You can dismiss and ignore this error.
5. Provide PowerProtect Data Manager administrator level credentials, and then click **OK**.
The dialog updates to indicate that the registration is in progress. If the vCenter Server does not trust the SSL certificate of the PowerProtect Data Manager server, a prompt displays to accept the certificate as trusted. You can trust this certificate, or alternatively, you can securely obtain a copy of the certificate as a file, and then click **Browse** within this prompt to select and trust the certificate. The vCenter documentation provides more information.
6. When the registration is complete, click **OK** to exit the **New Storage Provider** dialog.
The **Configure** tab updates to display the new VASA provider.

Results

You can now use the **vSphere Client** to create a virtual machine storage policy and associate this policy with an existing PowerProtect Data Manager virtual machine protection policy.


-  **NOTE:** If the provider goes offline at any point, you can select the provider in the table and click **Rescan** to reestablish a connection. Also, If the provider is removed and then readded, any policies that were previously assigned to the provider are restored.

Add an SPBM policy and associate with a PowerProtect Data Manager virtual machine policy

Use the **vSphere Client** to create a virtual machine storage policy and associate this policy with an existing PowerProtect Data Manager virtual machine protection policy.

Steps

1. In the **vSphere Client**, select the vCenter Server in the left pane.
2. Go to **Menu > Policies and Profiles**.
3. In the left pane, select **VM Storage Policies**, and then click **Create** in the right pane.
The **Create VM Storage Policy** wizard appears.
4. Provide a name and description that helps identify this policy as a storage policy that you want to associate with a PowerProtect Data Manager protection policy, and then click **Next**.
5. On the **Policy Structure** page, select **Enable host based rules**, and then click **Next**.
6. On the **Host based services** page, select the **Data Protection** tab, and then perform the following:
 - a. Select **Custom**.
 - b. From the **Provider** list, select **DellEMC PowerProtect** as the registered provider.
 - c. From the **PPDM Protection Policy** list, select an existing PowerProtect Data Manager virtual machine protection policy that you want to associate with this storage policy.

-  **NOTE:** Dell Technologies recommends that you use a descriptive name for the PowerProtect Data Manager virtual machine protection policy so that the purpose is easy to identify, since the **vSphere Client** does not provide policy

details within the **PowerProtect** portlet. If you decide to rename the PowerProtect Data Manager policy at any point, the association is retained since the UUID of the policy is used to create the connection.


d. Click **Next**.

7. Complete the storage policy details, and click **Finish**.

Results

The **VM Storage Policies** window displays the new storage policy in the table. An association is created between the PowerProtect Data Manager policy and the virtual machine storage policy, and the **PowerProtect** portlet in the **vSphere Client** updates to display the PowerProtect Data Manager protection policy. You can now perform manual backups and scheduled restores of the virtual assets in this policy.

When you assign the new storage policy to a virtual machine, that virtual machine should automatically be assigned to the associated PowerProtect Data Manager protection policy as well. Also, if you are creating a new virtual machine, you can assign a storage policy to the new virtual machine during this process.

 **NOTE:** You can create separate storage policies for each virtual machine disk, but only the policy that is associated with the virtual machine is used for data protection.

 **NOTE:** If you want to remove a virtual machine from protection, assign the virtual machine to a different policy, or to the Datastore Default policy.

Monitor virtual machine protection policy compliance

You can use the **Storage Policies** portlet within the **vSphere Client** to monitor the compliance of virtual assets in PowerProtect Data Manager virtual machine protection policies.

To access the portlet:

- Select the **Summary** tab, or
- Select the **Configure** tab, select a virtual machine in the left pane, and then click Policies.

If a virtual asset was unassigned from the policy within PowerProtect Data Manager, the policy displays as **Non-compliant**.

VMware Cloud (VMC) on Amazon Web Services (AWS)

Topics:

- PowerProtect Data Manager image backup and recovery
- Supported PowerProtect Data Manager and DDVE deployment configurations
- Deployment and configuration best practices and requirements
- Configuring the VMC-on-AWS portal
- Interoperability with PowerProtect Data Manager features
- vCenter server inventory requirements
- Creating a dedicated cloud-based vCenter user account
- Add a VM Direct Engine
- Unsupported operations

PowerProtect Data Manager image backup and recovery

PowerProtect Data Manager provides image backup and restore support for VMware Cloud (VMC) on Amazon Web Services (AWS).

Using PowerProtect Data Manager to protect virtual-machine assets in VMC on AWS is similar to how you protect virtual-machine assets in an on-premises data center. The following sections provide information on network configuration requirements, PowerProtect Data Manager best practices, and unsupported PowerProtect Data Manager operations.

Supported PowerProtect Data Manager and DDVE deployment configurations

In order to protect virtual-machine assets in VMC on AWS, PowerProtect Data Manager and DDVE can be deployed in several ways.

When deploying PowerProtect Data Manager and DDVE, two possible deployment environments are VMware Cloud on AWS (VMC on AWS) and the AWS Marketplace (AWS). The following table describes the supported deployment configurations of the two products:

Table 45. Supported deployment configurations

PowerProtect Data Manager	DDVE
VMware Cloud on AWS	VMware Cloud on AWS
VMware Cloud on AWS	AWS Marketplace
AWS Marketplace	AWS Marketplace

When deploying PowerProtect Data Manager to VMC on AWS, an Open Virtualization Appliance (OVA) is used. This puts PowerProtect Data Manager into the VMC-on-AWS environment in order to protect the VMware assets. When deploying PowerProtect Data Manager to AWS, a machine image is used. This puts PowerProtect Data Manager into a cloud-marketplace environment, but still allows the VMware assets in the VMC-on-AWS environment to be protected.

For more information about the different deployment types, see the *PowerProtect Data Manager Deployment Guide* and the *PowerProtect Data Manager AWS Deployment Guide*.

Deployment and configuration best practices and requirements

Deploying and configuring PowerProtect Data Manager, DDVE, and other components in a certain way provides an efficient protection of virtual-machine assets.

To perform data protection and disaster recovery tasks in VMC on AWS, consider the following recommendations for the backup infrastructure:

- Deploy PowerProtect Data Manager and DDVE either to VMC on AWS or to AWS.
- Deploy the VM Direct appliance to VMC on AWS.
- Deploy at least one VM Direct appliance for each software-defined data center (SDDC) cluster in the VMC-on-AWS environment.
- When deploying or configuring PowerProtect Data Manager or the VM Direct appliance, ensure that the DNS server IP points to the internal DNS server that is running in vCenter inventory.
- Ensure that the internal DNS server has both forward and reverse lookup entries for all of the required components, such as the PowerProtect Data Manager server, the 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, perform one of the following actions:
 - Specify the login credentials for the `cloudadmin@vmc.local` user.
 - Refer to [Creating a dedicated cloud-based vCenter user account](#) on page 193 to create a dedicated cloud-based vCenter user account, and then specify the login credentials for that user.
- You can clone backups to another instance of DDVE running in the same environment as the first instance. 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.
- You can store backups outside of the VMC-on-AWS environment. For example, store backups on an AWS virtual private cloud (VPC). This type of deployment enables efficient data transfer over the fast ENI connection that is used by VMware to communicate with AWS.

Configuring the VMC-on-AWS portal

Domain Name System (DNS) resolution is critical for deployment and configuration of PowerProtect Data Manager, the PowerProtect Data Manager external proxy, and DDVE. 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.

Ensure that the VMC-on-AWS portal meets the following requirements:

- By default, there is no external access to the vCenter server in the software-defined data center (SDDC). You can open access to the vCenter server 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 VMC 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 to which the PowerProtect Data Manager server virtual machine is connected.
- Configure DNS to allow machines in the SDDC to resolve FQDNs to their public IP addresses. If the DNS server is not configured in the SDDC, the PowerProtect Data Manager 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 DD system as a virtual appliance. If deploying DDVE to VMC-on-AWS, connect the SDDC to an AWS account during the SDDC creation, and then select a VPC and subnet within that account.
- DDVE must be connected to the SDDC through the VMC-on-AWS Elastic Network Interfaces (ENIs). This action allows the SDDC, the services in the 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 DDVE.

For more information about configuring ENIs, see <https://vmc.vmware.com/console/aws-link>.

- If DDVE is running in VMC-on-AWS, configure the inbound and outbound firewall rules of the compute gateway for DDVE connectivity.

For detailed information on what incoming and outgoing ports need to be opened for PowerProtect-VM proxy solution, refer to the *PowerProtect Data Manager Security Configuration Guide*.

- If using NSX-T, configure DNS to resolve to the internal IP address of the vCenter server. Navigate to **SDDC Management > Settings > vCenter FQDN**, and then select the **Private vCenter IP address** to directly access the management network over the built-in firewall.
- Open TCP port 443 of the vCenter and ESXi servers in both the management and compute gateways.
- If DDVE is running in VMC-on-AWS, the inbound and outbound firewall rules of the VMC-on-AWE VPC security group are configured to provide connectivity between the SDDC compute gateway and DDVE.
- If there is replication between DDVE instances, ensure the following:
 - The security group in AWS is configured to allow all inbound traffic from the private IPs of the DDVE instances
 - The DDVE instances can ping each other using their FQDNs

Interoperability with PowerProtect Data Manager features

VMC 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 following non-accessible areas:

- vSAN datastore 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 the SDDC, ensure that the following requirements are met:

- An internal DNS name server must be running inside vCenter inventory. This will be referenced by all the workloads running in the 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 itself cannot resolve.

Creating a dedicated cloud-based vCenter user account

It is recommended that you set up a separate vCenter user account at the root level of the vCenter hierarchy. This account is strictly dedicated for use with PowerProtect Data Manager and the VM Direct protection engine in cloud-based environments.

Use of a generic user account such as **Administrator** could 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 a vCenter user account when you add the vCenter server as an asset source in the user interface. When you add the vCenter server, ensure that you specify a user whose cloud-based role is defined at the vCenter level and not restricted to a lower-level container object in the vSphere object hierarchy.

Specify the required privileges for a dedicated cloud-based vCenter user account

You can use the **vSphere Client** to specify the required privileges for the dedicated cloud-based 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.

NOTE: For the privileges required when administering on-premises PowerProtect Data Manager, see [Specify the required privileges for a dedicated vCenter user account](#) on page 64.

Table 46. Minimum required cloud-based vCenter user account privileges



Setting	vCenter 6.0 and later required privileges	PowerCLI equivalent required privileges
Alarms	<ul style="list-style-type: none">Create alarmModify alarm	<pre>\$privileges = @('System.Anonymous', 'System.View', 'System.Read', 'Alarm.Create', 'Alarm.Edit', 'Cryptographer.Access', 'Datastore.Browse', 'Datastore.DeleteFile', 'Datastore.FileManagement', 'Datastore.AllocateSpace', 'Datastore.Config', 'Folder.Create', 'Global.ManageCustomFields', 'Global.SetCustomField', 'Global.LogEvent', 'Global.CancelTask', 'InventoryService.Tagging.AttachTag', 'InventoryService.Tagging.ObjectAttachable', 'InventoryService.Tagging.CreateTag', 'InventoryService.Tagging.CreateCategory', 'Network.Assign', 'Resource.AssignVMToPool', 'Resource.HotMigrate', 'Resource.ColdMigrate', 'Sessions.ValidateSession', 'StorageProfile.View', 'VApp.ApplicationConfig', 'VApp.Export', 'VApp.Import', '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.GuestOperations.Query', 'VirtualMachine.GuestOperations.Modify', 'VirtualMachine.GuestOperations.Execute', 'VirtualMachine.Interact.PowerOn', 'VirtualMachine.Interact.PowerOff',</pre>
Cryptographic operations	<ul style="list-style-type: none">Direct Access <div> NOTE: This only applies to AVS and GCVE.</div>	
Datastore	<ul style="list-style-type: none">Allocate spaceBrowse datastoreConfigure datastoreLow level file operationsRemove file	
Folder	<ul style="list-style-type: none">Create folder	
Global	<ul style="list-style-type: none">Cancel taskLog eventManage custom attributesSet custom attribute	
vSphere Tagging	<ul style="list-style-type: none">Assign or Unassign vSphere TagAssign or Unassign vSphere Tag on Object <div> NOTE: This only applies to vCenter 7.0 and later.</div> <ul style="list-style-type: none">Create vSphere TagCreate vSphere Tag Category	
Network	<ul style="list-style-type: none">Assign network	
Resource	<ul style="list-style-type: none">Assign virtual machine to resource poolMigrate powered off virtual machineMigrate powered on virtual machine	
Sessions	<ul style="list-style-type: none">Validate session	
SPBM policy restore	<ul style="list-style-type: none">Profile-driven storage view	
vApp	<ul style="list-style-type: none">ExportImportvApp application configuration	
Virtual Machine		
Change Configuration	<ul style="list-style-type: none">Acquire disk leaseAdd existing diskAdd new diskAdd or remove deviceAdvanced configurationChange CPU countChange MemoryChange SettingsChange Swapfile placementChange resourceConfigure Host USB deviceConfigure Raw deviceConfigure managedby	

Table 46. Minimum required cloud-based vCenter user account privileges (continued)

Setting	vCenter 6.0 and later required privileges	PowerCLI equivalent required privileges
	<ul style="list-style-type: none"> Extend virtual disk Modify device settings Reload from path Remove disk Rename Reset guest information Set annotation Toggle disk change tracking Upgrade virtual machine compatibility 	<pre>'VirtualMachine.Interact.Reset', 'VirtualMachine.Interact.ConsoleInteract', 'VirtualMachine.Interact.DeviceConnecti on', 'VirtualMachine.Interact.SetCDMedia', 'VirtualMachine.Interact.ToolsInstall', 'VirtualMachine.Interact.GuestControl', 'VirtualMachine.Inventory.Create', 'VirtualMachine.Inventory.Register', 'VirtualMachine.Inventory.Delete', 'VirtualMachine.Inventory.Unregister', 'VirtualMachine.Provisioning.DiskRandom Access', 'VirtualMachine.Provisioning.DiskRandom Read', 'VirtualMachine.Provisioning.GetVmFiles ', 'VirtualMachine.Provisioning.MarkAsTemp late', 'VirtualMachine.State.CreateSnapshot', 'VirtualMachine.State.RevertToSnapshot' , 'VirtualMachine.State.RemoveSnapshot')</pre>
Edit Inventory	<ul style="list-style-type: none"> Create new Register Remove Unregister 	
Guest operations	<ul style="list-style-type: none"> Guest operation modifications Guest operation program execution Guest operation queries 	
Interaction	<ul style="list-style-type: none"> Configure CD media Connect devices Console interaction Guest operating system management by VIX API Install VMware Tools Power off Power on Reset 	<pre>New-VIRole -Name 'PowerProtect' -Privilege (Get-VIPrivilege -Id \$privileges)</pre>
Provisioning	<ul style="list-style-type: none"> Allow disk access Allow read-only disk access Allow virtual machine download Mark as template 	
Snapshot Management	<ul style="list-style-type: none"> Create snapshot Remove snapshot Revert to snapshot 	

Add a VM Direct Engine

Perform the following steps in the **Protection Engines** window of the PowerProtect Data Manager UI to deploy an external VM Direct Engine, also referred to as a VM proxy. The VM Direct Engine facilitates data movement for virtual-machine protection policies.

Prerequisites

Review the sections [Requirements for an external VM Direct Engine](#) on page 66 and [Transport mode considerations](#) on page 252.


If applicable, complete all of the virtual network configuration tasks before you assign any virtual networks.

About this task


The PowerProtect Data Manager software comes 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 you deploy external proxies by adding a VM Direct Engine for the following reasons:

- An external VM Direct Engine for VM proxy backup and recovery can provide improved performance and reduce network bandwidth utilization by using source-side deduplication.

- The embedded VM Direct engine has limited capacity for backup streams.
- The embedded VM Direct engine is not supported for VMC-on-AWS, AVS-on-Azure, or GCVE-on-GCP operations.

 **NOTE:** Cloud-based deployments of PowerProtect Data Manager do not support the configuration of data-traffic routing or VLANs. Skip the **Networks Configuration** page.


Steps

1. From the left navigation pane, select **Infrastructure > Protection Engines**.
The **Protection Engines** window appears.
2. In the **VM Direct Engines** pane of the **Protection Engines** window, click **Add**.
The **Add Protection Engine** wizard displays.
3. On the **Protection Engine Configuration** page, complete the required fields, which are marked with an asterisk.
 - **Hostname, Gateway, IP Address, Netmask, and Primary DNS**—Note that only IPv4 addresses are supported.
 - **vCenter to Deploy**—If you have added multiple vCenter Server instances, select the vCenter on which to deploy the protection engine.
 **NOTE:** Ensure that you do not select the internal vCenter Server.
 - **ESX Host/Cluster**—Select on which cluster or ESXi host you want to deploy the protection engine.
 - **Network**—Displays all the networks that are available under the selected ESXi Host/Cluster. For virtual networks (VLANs), this network carries management traffic.
 - **Data Store**—Displays all datastores that are accessible to the selected ESXi Host/Cluster based on ranking (whether the datastores are shared or local), 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 protection engine resides, or leave the default selection of **<automatic>** to allow PowerProtect Data Manager to determine the best location to host the protection engine.
 - **Transport Mode**—Select **Hot Add**.
 - **Supported Protection Type**—Select whether this protection engine is intended for **Virtual Machine, Kubernetes** Tanzu guest cluster, or **NAS** asset protection.
4. Click **Next**.
5. Click **Next** to skip the **Networks Configuration** page..
6. On the **Summary** page, review the information and then click **Finish**.
The protection engine is added to the **VM Direct Engines** pane. An additional column indicates the engine purpose. Note that it can take several minutes to register the new protection engine in PowerProtect Data Manager. The protection engine also appears in the **vSphere Client**.

Results

When an external VM Direct Engine is deployed and registered, PowerProtect Data Manager uses this engine instead of the embedded VM Direct engine for any data protection operations that involve virtual machine protection policies. If every external VM Direct Engine is unavailable, PowerProtect Data Manager uses the embedded VM Direct engine as a fallback to perform limited scale backups and restores. If you do not want to use the external VM Direct Engine, you can disable this engine. [Additional VM Direct actions](#) on page 68 provides more information.

 **NOTE:** The external VM Direct Engine is always required for VMC-on-AWS, AVS-on-Azure, and GCVE-on-GCP operations. If no external VM Direct Engine is available for these solutions, data protection operations fail.

Next steps


If the protection engine 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, delete the failed protection engine and then add the protection engine in the **Protection Engines** window.

When configuring the VM Direct Engine in a VMC-on-AWS, AVS-on-Azure, or GCVE-on-GCP environment, if you deploy the VM Direct Engine to the root of the cluster instead of inside the Compute-ResourcePool, you must move the VM Direct Engine inside the Compute-ResourcePool.

Unsupported operations

PowerProtect Data Manager image backup and restore in VMC on AWS does not currently support the following operations:

- PowerProtect Search functionality
- The vSphere Storage Policy Based Management (SPBM) integration with PowerProtect Data Manager
- A VM Direct appliance that is configured with dual-stack or IPv6
- Application-consistent data protection for Microsoft SQL with the VM Direct appliance
- VM Backup and Recovery HTML5 plug-in functionality for vSphere
- Image-based backups and restores that use NBD or the NBDSSL transport mode
- Image-based backups and restores when a datacenter is placed inside a folder in the SDDC
- File-level recoveries of an image-based backup
- Instant-access restores of an image-based backup
- Emergency restores of an image-based restore directly to an ESXi host, bypassing the vCenter server
- Backup and restore operations with anything other than the **CloudAdmin** role or a customized role that has all of the privileges listed in [Specify the required privileges for a dedicated cloud-based vCenter user account](#) on page 193

 **NOTE:** If protecting virtual-machine assets with a PowerProtect Data Manager machine image deployed to AWS, Cloud Disaster Recovery (CDR) and Search Clusters are also unsupported.

Azure VMware Solution (AVS) on Microsoft Azure

Topics:

- [PowerProtect Data Manager image backup and recovery](#)
- [Supported PowerProtect Data Manager and DDVE deployment configurations](#)
- [Deployment and configuration best practices and requirements](#)
- [Configuring the AVS-on-Azure portal](#)
- [vCenter server inventory requirements](#)
- [Creating a dedicated cloud-based vCenter user account](#)
- [Add a VM Direct Engine](#)
- [Unsupported operations](#)

PowerProtect Data Manager image backup and recovery

PowerProtect Data Manager provides image backup and restore support for Azure VMware Solution (AVS) on Microsoft Azure.

Using PowerProtect Data Manager to protect virtual-machine assets AVS on Azure is similar to how you protect virtual-machine assets in an on-premises data center. This section provides information on network configuration requirements, PowerProtect Data Manager best practices, and unsupported PowerProtect Data Manager operations.

Supported PowerProtect Data Manager and DDVE deployment configurations

In order to protect virtual-machine assets in AVS on Azure, PowerProtect Data Manager and DDVE can be deployed in a couple of ways.

When deploying PowerProtect Data Manager and DDVE, two possible deployment environments are Azure VMware Solution (AVS on Azure) and the Azure Marketplace (Azure). The following table describes the supported deployment configurations of the two products:

Table 47. Supported deployment configurations

PowerProtect Data Manager	DDVE
Azure VMware Solution	Azure Marketplace
Azure Marketplace	Azure Marketplace

When deploying PowerProtect Data Manager to AVS on Azure, an Open Virtualization Appliance (OVA) is used. This puts PowerProtect Data Manager into the AVS-on-Azure environment in order to protect the VMware assets. When deploying PowerProtect Data Manager to Azure, a machine image is used. This puts PowerProtect Data Manager into a cloud-marketplace environment, but still allows the VMware assets in the AVS-on-Azure environment to be protected.

For more information about the different deployment types, see the *PowerProtect Data Manager Deployment Guide* and the *PowerProtect Data Manager Azure Deployment Guide*.

Deployment and configuration best practices and requirements

Deploying and configuring PowerProtect Data Manager, DDVE, and other components in a certain way provides an efficient protection of virtual-machine assets.

To perform data protection and disaster recovery tasks in AVS on Azure, consider the following recommendations and requirements for the backup infrastructure:

- Deploy PowerProtect Data Manager either to AVS on Azure or to Azure.
- Deploy DDVE to Azure.
- Deploy the VM Direct appliance to AVS on Azure. Deploy at least one VM Direct appliance for each software-defined data center (SDDC) cluster in the AVS-on-Azure environment.
- When deploying or configuring PowerProtect Data Manager or the VM Direct appliance, ensure that the DNS server IP points to the internal DNS server that is running in vCenter inventory.
- Ensure that the internal DNS server has both forward and reverse lookup entries for all of the required components, such as the PowerProtect Data Manager server, the VM Direct appliance, and DDVE.
- 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, perform one of the following actions:
 - Specify the login credentials for the `cloudadmin@vsphere.local` user.
 - Refer to [Creating a dedicated cloud-based vCenter user account](#) on page 193 to create a dedicated cloud-based vCenter user account, and then specify the login credentials for that user.
- You can clone backups to another instance of DDVE running in Azure. This type of deployment enables backup copies to be stored for longer retention, leveraging the Azure network for transferring data at lower latency and cost when compared to the public Internet.

Configuring the AVS-on-Azure portal

Domain Name System (DNS) resolution is critical for deployment and configuration of PowerProtect Data Manager, the PowerProtect Data Manager external proxy, and the DDVE 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.

Ensure that the AVS-on-Azure portal meets the following requirements:

- If you have deployed a PowerProtect Data Manager OVA to AVS on Azure or a PowerProtect Data Manager machine image to Azure, it is configured to use a custom DNS server.
 - NOTE:** If you have already deployed PowerProtect Data Manager without a custom DNS server, you will have to redeploy it. For more information, see the *PowerProtect Data Manager Deployment Guide* or the *PowerProtect Data Manager Azure Deployment Guide*.
- Forward and reverse DNS lookups exist for PowerProtect Data Manager, vCenter, DDVE, ESXi, and each VM Direct Engine.
- DNS is configured to allow machines in the SDDC to resolve FQDNs to their IP addresses.
- DDVE is running in Azure. If you have more than one DDVE instance running in Azure to perform replication, the DDVE instances have the ability to ping each other using their FQDNs.
 - NOTE:** DDVE running in AVS-on-Azure is not supported.
- DDVE has DNS entries for PowerProtect Data Manager and each VM Direct Engine.
- SDDC is connected to an Azure account, and an Azure cloud and subnet within that account is selected.
- Any DDVE instance on Azure is connected to the SDDC through a Vnet. This action allows the SDDC, the services in the Azure cloud, and subnets in the Azure account to communicate without having to route traffic through the Internet gateway.

The same Vnets are recommended for access to DDVE instances. For more information about configuring Vnets, see [About Virtual Network](#).

vCenter server inventory requirements

In the vCenter server inventory of the SDDC, ensure that the following requirements are met:

- An internal DNS name server must be running inside vCenter inventory. This will be referenced by all the workloads running in the 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 itself cannot resolve.

Creating a dedicated cloud-based vCenter user account

It is recommended that you set up a separate vCenter user account at the root level of the vCenter hierarchy. This account is strictly dedicated for use with PowerProtect Data Manager and the VM Direct protection engine in cloud-based environments.

Use of a generic user account such as **Administrator** could 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 a vCenter user account when you add the vCenter server as an asset source in the user interface. When you add the vCenter server, ensure that you specify a user whose cloud-based role is defined at the vCenter level and not restricted to a lower-level container object in the vSphere object hierarchy.

Specify the required privileges for a dedicated cloud-based vCenter user account

You can use the **vSphere Client** to specify the required privileges for the dedicated cloud-based 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.


 **NOTE:** For the privileges required when administering on-premises PowerProtect Data Manager, see [Specify the required privileges for a dedicated vCenter user account](#) on page 64.

Table 48. Minimum required cloud-based vCenter user account privileges


Setting	vCenter 6.0 and later required privileges	PowerCLI equivalent required privileges
Alarms	<ul style="list-style-type: none">• Create alarm• Modify alarm	<pre>\$privileges = @('System.Anonymous', 'System.View', 'System.Read', 'Alarm.Create', 'Alarm.Edit', 'Cryptographer.Access', 'Datastore.Browse', 'Datastore.DeleteFile', 'Datastore.FileManagement', 'Datastore.AllocateSpace', 'Datastore.Config', 'Folder.Create', 'Global.ManageCustomFields', 'Global.SetCustomField', 'Global.LogEvent', 'Global.CancelTask', 'InventoryService.Tagging.AttachTag', 'InventoryService.Tagging.ObjectAttachable', 'InventoryService.Tagging.CreateTag', 'InventoryService.Tagging.CreateCategory',</pre>
Cryptographic operations	<ul style="list-style-type: none">• Direct Access <p> NOTE: This only applies to AVS and GCVE.</p>	
Datastore	<ul style="list-style-type: none">• Allocate space• Browse datastore• Configure datastore• Low level file operations• Remove file	
Folder	<ul style="list-style-type: none">• Create folder	
Global	<ul style="list-style-type: none">• Cancel task• Log event• Manage custom attributes• Set custom attribute	
vSphere Tagging	<ul style="list-style-type: none">• Assign or Unassign vSphere Tag	

Table 48. Minimum required cloud-based vCenter user account privileges (continued)

Setting	vCenter 6.0 and later required privileges	PowerCLI equivalent required privileges
	<ul style="list-style-type: none"> Assign or Unassign vSphere Tag on Object <p>NOTE: This only applies to vCenter 7.0 and later.</p> <ul style="list-style-type: none"> Create vSphere Tag Create vSphere Tag Category 	'Network.Assign', 'Resource.AssignVMToPool', 'Resource.HotMigrate', 'Resource.ColdMigrate', 'Sessions.ValidateSession', 'StorageProfile.View', 'VApp.ApplicationConfig', 'VApp.Export', 'VApp.Import', '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.GuestOperations.Query', 'VirtualMachine.GuestOperations.Modify', 'VirtualMachine.GuestOperations.Execute', '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.Inventory.Create', 'VirtualMachine.Inventory.Register', 'VirtualMachine.Inventory.Delete', 'VirtualMachine.Inventory.Unregister', 'VirtualMachine.Provisioning.DiskRandomAccess', 'VirtualMachine.Provisioning.DiskRandomRead', 'VirtualMachine.Provisioning.GetVmFiles', 'VirtualMachine.Provisioning.MarkAsTemplate', 'VirtualMachine.State.CreateSnapshot', 'VirtualMachine.State.RevertToSnapshot', 'VirtualMachine.State.RemoveSnapshot',)
Network	<ul style="list-style-type: none"> Assign network 	
Resource	<ul style="list-style-type: none"> Assign virtual machine to resource pool Migrate powered off virtual machine Migrate powered on virtual machine 	
Sessions	<ul style="list-style-type: none"> Validate session 	
SPBM policy restore	<ul style="list-style-type: none"> Profile-driven storage view 	
vApp	<ul style="list-style-type: none"> Export Import vApp application configuration 	
Virtual Machine		
Change Configuration	<ul style="list-style-type: none"> Acquire disk lease Add existing disk Add new disk Add or remove device Advanced configuration Change CPU count Change Memory Change Settings Change Swapfile placement Change resource Configure Host USB device Configure Raw device Configure managedby Extend virtual disk Modify device settings Reload from path Remove disk Rename Reset guest information Set annotation Toggle disk change tracking Upgrade virtual machine compatibility 	
Edit Inventory	<ul style="list-style-type: none"> Create new Register Remove Unregister 	
Guest operations	<ul style="list-style-type: none"> Guest operation modifications Guest operation program execution Guest operation queries 	
Interaction	<ul style="list-style-type: none"> Configure CD media Connect devices Console interaction 	

Table 48. Minimum required cloud-based vCenter user account privileges (continued)

Setting	vCenter 6.0 and later required privileges	PowerCLI equivalent required privileges
	<ul style="list-style-type: none"> Guest operating system management by VIX API Install VMware Tools Power off Power on Reset 	<pre>-Privilege (Get-VIPrivilege -Id \$privileges)</pre>
Provisioning	<ul style="list-style-type: none"> Allow disk access Allow read-only disk access Allow virtual machine download Mark as template 	
Snapshot Management	<ul style="list-style-type: none"> Create snapshot Remove snapshot Revert to snapshot 	

Add a VM Direct Engine

Perform the following steps in the **Protection Engines** window of the PowerProtect Data Manager UI to deploy an external VM Direct Engine, also referred to as a VM proxy. The VM Direct Engine facilitates data movement for virtual-machine protection policies.

Prerequisites


Review the sections [Requirements for an external VM Direct Engine](#) on page 66 and [Transport mode considerations](#) on page 252.

If applicable, complete all of the virtual network configuration tasks before you assign any virtual networks.


About this task

The PowerProtect Data Manager software comes 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 you deploy external proxies by adding a VM Direct Engine for the following reasons:

- An external VM Direct Engine for VM proxy backup and recovery can provide improved performance and reduce network bandwidth utilization by using source-side deduplication.
- The embedded VM Direct engine has limited capacity for backup streams.
- The embedded VM Direct engine is not supported for VMC-on-AWS, AVS-on-Azure, or GCVE-on-GCP operations.

 **NOTE:** Cloud-based deployments of PowerProtect Data Manager do not support the configuration of data-traffic routing or VLANs. Skip the **Networks Configuration** page.

Steps

1. From the left navigation pane, select **Infrastructure > Protection Engines**.
The **Protection Engines** window appears.
2. In the **VM Direct Engines** pane of the **Protection Engines** window, click **Add**.
The **Add Protection Engine** wizard displays.
3. On the **Protection Engine Configuration** page, complete the required fields, which are marked with an asterisk.
 - **Hostname, Gateway, IP Address, Netmask, and Primary DNS**—Note that only IPv4 addresses are supported.
 - **vCenter to Deploy**—If you have added multiple vCenter Server instances, select the vCenter on which to deploy the protection engine.
 **NOTE:** Ensure that you do not select the internal vCenter Server.
 - **ESX Host/Cluster**—Select on which cluster or ESXi host you want to deploy the protection engine.
 - **Network**—Displays all the networks that are available under the selected ESXi Host/Cluster. For virtual networks (VLANs), this network carries management traffic.

- **Data Store**—Displays all datastores that are accessible to the selected ESXi Host/Cluster based on ranking (whether the datastores are shared or local), 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 protection engine resides, or leave the default selection of **<automatic>** to allow PowerProtect Data Manager to determine the best location to host the protection engine.

- **Transport Mode**—Select **Hot Add**.
- **Supported Protection Type**—Select whether this protection engine is intended for **Virtual Machine**, **Kubernetes** Tanzu guest cluster, or **NAS** asset protection.

4. Click **Next**.
5. Click **Next** to skip the **Networks Configuration** page..
6. On the **Summary** page, review the information and then click **Finish**.

The protection engine is added to the **VM Direct Engines** pane. An additional column indicates the engine purpose. Note that it can take several minutes to register the new protection engine in PowerProtect Data Manager. The protection engine also appears in the **vSphere Client**.

Results

When an external VM Direct Engine is deployed and registered, PowerProtect Data Manager uses this engine instead of the embedded VM Direct engine for any data protection operations that involve virtual machine protection policies. If every external VM Direct Engine is unavailable, PowerProtect Data Manager uses the embedded VM Direct engine as a fallback to perform limited scale backups and restores. If you do not want to use the external VM Direct Engine, you can disable this engine.

[Additional VM Direct actions](#) on page 68 provides more information.

NOTE: The external VM Direct Engine is always required for VMC-on-AWS, AVS-on-Azure, and GCVE-on-GCP operations. If no external VM Direct Engine is available for these solutions, data protection operations fail.

Next steps

If the protection engine 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, delete the failed protection engine and then add the protection engine in the **Protection Engines** window.

When configuring the VM Direct Engine in a VMC-on-AWS, AVS-on-Azure, or GCVE-on-GCP environment, if you deploy the VM Direct Engine to the root of the cluster instead of inside the Compute-ResourcePool, you must move the VM Direct Engine inside the Compute-ResourcePool.

Unsupported operations

PowerProtect Data Manager image backup and restore in AVS on Azure does not currently support the following operations:

- PowerProtect Search functionality
- A VM Direct appliance that is configured with dual-stack or IPv6
- Application-consistent data protection for Microsoft SQL with the VM Direct appliance
- VM Backup and Recovery HTML5 plug-in functionality for vSphere
- Image-based backups and restores that use NBD or the NBDSSL transport mode
- Image-based backups and restores when a datacenter is placed inside a folder in the SDDC
- File-level recoveries of an image-based backup
- Instant-access restores of an image-based backup
- Emergency restores of an image-based restore directly to an ESXi host, bypassing the vCenter server
- Backup and restore operations with anything other than the **CloudAdmin** role or a customized role that has all of the privileges listed in [Specify the required privileges for a dedicated cloud-based vCenter user account](#) on page 193

NOTE: If protecting virtual-machine assets with a PowerProtect Data Manager machine image deployed to Azure, Cloud Disaster Recovery (CDR), Search Clusters, and Microsoft Exchange are also unsupported.

Google Cloud VMware Engine (GCVE) on Google Cloud Product (GCP)

Topics:

- PowerProtect Data Manager image backup and recovery
- Supported PowerProtect Data Manager and DDVE deployment configurations
- Deployment and configuration best practices and requirements
- Configuring the GCVE-on-GCP portal
- vCenter server inventory requirements
- Creating a dedicated cloud-based vCenter user account
- Add a VM Direct Engine
- Unsupported operations

PowerProtect Data Manager image backup and recovery

PowerProtect Data Manager provides image backup and restore support for Google Cloud VMware Engine (GCVE) on Google Cloud Platform (GCP).

Using PowerProtect Data Manager to protect virtual-machine assets in GCVE on GCP is similar to how you protect virtual-machines assets in an on-premises data center. The following sections provide information on network configuration requirements, PowerProtect Data Manager best practices, and unsupported PowerProtect Data Manager operations.

Supported PowerProtect Data Manager and DDVE deployment configurations

In order to protect virtual-machine assets in GCVE on GCP, PowerProtect Data Manager and DDVE can be deployed in a couple of ways.

When deploying PowerProtect Data Manager and DDVE, two possible deployment environments are Google Cloud VMware Engine (GCVE on GCP) and the Google Cloud Marketplace (GCP). The following table describes the supported deployment configurations of the two products:

Table 49. Supported deployment configurations

PowerProtect Data Manager	DDVE
Google Cloud VMware Engine	Google Cloud Marketplace
Google Cloud Marketplace	Google Cloud Marketplace

When deploying PowerProtect Data Manager to GCVE on GCP, an Open Virtualization Appliance (OVA) is used. This puts PowerProtect Data Manager into the GCVE-on-GCP environment in order to protect the VMware assets. When deploying PowerProtect Data Manager to GCP, a machine image is used. This puts PowerProtect Data Manager into a cloud-marketplace environment, but still allows the VMware assets in the GCVE-on-GCP environment to be protected.

For more information about the different deployment types, see the *PowerProtect Data Manager Deployment Guide* and the *PowerProtect Data Manager GCP Deployment Guide*.

Deployment and configuration best practices and requirements

For GCVE-on GCP support, ensure that the following requirements are met:

To perform data protection and disaster recovery tasks in GCVE on GCP, consider the following recommendations and requirements for the backup infrastructure deployment:

- Deploy PowerProtect Data Manager either to GCVE on GCP or to GCP.
- Deploy DDVE to GCP.
- Deploy the VM Direct appliance in a GCVE-on-GCP environment. Deploy at least one VM Direct appliance for each software-defined data center (SDDC) cluster in GCVE on GCP.
- When deploying or configuring PowerProtect Data Manager or the VM Direct appliance, ensure that the DNS server IP points to the internal DNS server that is running in vCenter inventory.
- Ensure that the internal DNS server has both forward and reverse lookup entries for all of the required components, such as the PowerProtect Data Manager server, the VM Direct appliance, and DDVE.
- 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, perform one of the following actions:
 - Specify the login credentials for the *CloudOwner@gve.local* user.
 - Refer to the following section to create a dedicated cloud-based vCenter user account, and then specify the login credentials for that user.
- You can clone backups to another DDVE instance running in GCP. This type of deployment enables backup copies to be stored for longer retention, leveraging the GCP network for transferring data at lower latency and cost when compared to the public Internet.

Configuring the GCVE-on-GCP portal

Domain Name System (DNS) resolution is critical for deployment and configuration of PowerProtect Data Manager, the PowerProtect Data Manager external proxy, and DDVE. 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.

Ensure that the GCVE-on-GCP portal meets the following requirements:

- If you have deployed a PowerProtect Data Manager OVA to GVCE on GCP or a PowerProtect Data Manager machine image to GCP, it is configured to use a custom DNS server.
 - NOTE:** If you have already deployed PowerProtect Data Manager without a custom DNS server, you will have to redeploy it. For more information, see the *PowerProtect Data Manager Deployment Guide* or the *PowerProtect Data Manager GCP Deployment Guide*.
- Forward and reverse DNS lookups exist for PowerProtect Data Manager, vCenter, DDVE, ESXi, and each VM Direct Engine.
- DNS is configured to allow machines in the SDDC to resolve FQDNs to their IP addresses.
- DDVE is running in GCP. If you have more than one DDVE instance running in GCP to perform replication, both DDVE instances have the ability to ping each other using their FQDNs.
 - NOTE:** DDVE running in GCVE on GCP is not supported.
- DDVE has DNS entries for PowerProtect Data Manager and each VM Direct Engine.
- SDDC is connected to a Google account, and a Google cloud and subnet within that account is selected.
- Any DDVE instances running in GCP is connected to the SDDC through a Vnet. This action allows the SDDC, the services in GCP, and subnets in GCP to communicate without having to route traffic through the Internet gateway.

The same Vnet is recommended for access to DDVE instances. For more information about configuring Vnets, see [About Virtual Network](#).

vCenter server inventory requirements

In the vCenter server inventory of the SDDC, ensure that the following requirements are met:

- An internal DNS name server must be running inside vCenter inventory. This will be referenced by all the workloads running in the 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 itself cannot resolve.

Creating a dedicated cloud-based vCenter user account

It is recommended that you set up a separate vCenter user account at the root level of the vCenter hierarchy. This account is strictly dedicated for use with PowerProtect Data Manager and the VM Direct protection engine in cloud-based environments.

Use of a generic user account such as **Administrator** could 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 a vCenter user account when you add the vCenter server as an asset source in the user interface. When you add the vCenter server, ensure that you specify a user whose cloud-based role is defined at the vCenter level and not restricted to a lower-level container object in the vSphere object hierarchy.

Specify the required privileges for a dedicated cloud-based vCenter user account

You can use the **vSphere Client** to specify the required privileges for the dedicated cloud-based 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.


 **NOTE:** For the privileges required when administering on-premises PowerProtect Data Manager, see [Specify the required privileges for a dedicated vCenter user account](#) on page 64.

Table 50. Minimum required cloud-based vCenter user account privileges


Setting	vCenter 6.0 and later required privileges	PowerCLI equivalent required privileges
Alarms	<ul style="list-style-type: none">• Create alarm• Modify alarm	<pre>\$privileges = @('System.Anonymous', 'System.View', 'System.Read', 'Alarm.Create', 'Alarm.Edit', 'Cryptographer.Access', 'Datastore.Browse', 'Datastore.DeleteFile', 'Datastore.FileManagement', 'Datastore.AllocateSpace', 'Datastore.Config', 'Folder.Create', 'Global.ManageCustomFields', 'Global.SetCustomField', 'Global.LogEvent', 'Global.CancelTask', 'InventoryService.Tagging.AttachTag', 'InventoryService.Tagging.ObjectAttachable', 'InventoryService.Tagging.CreateTag', 'InventoryService.Tagging.CreateCategory',</pre>
Cryptographic operations	<ul style="list-style-type: none">• Direct Access <p> NOTE: This only applies to AVS and GCVE.</p>	
Datastore	<ul style="list-style-type: none">• Allocate space• Browse datastore• Configure datastore• Low level file operations• Remove file	
Folder	<ul style="list-style-type: none">• Create folder	
Global	<ul style="list-style-type: none">• Cancel task• Log event• Manage custom attributes• Set custom attribute	
vSphere Tagging	<ul style="list-style-type: none">• Assign or Unassign vSphere Tag	

Table 50. Minimum required cloud-based vCenter user account privileges (continued)

Setting	vCenter 6.0 and later required privileges	PowerCLI equivalent required privileges
	<ul style="list-style-type: none"> Assign or Unassign vSphere Tag on Object <p>NOTE: This only applies to vCenter 7.0 and later.</p> <ul style="list-style-type: none"> Create vSphere Tag Create vSphere Tag Category 	<pre>'Network.Assign', 'Resource.AssignVMToPool', 'Resource.HotMigrate', 'Resource.ColdMigrate', 'Sessions.ValidateSession', 'StorageProfile.View', 'VApp.ApplicationConfig', 'VApp.Export', 'VApp.Import', '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.GuestOperations.Query', 'VirtualMachine.GuestOperations.Modify', 'VirtualMachine.GuestOperations.Execute', '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.Inventory.Create', 'VirtualMachine.Inventory.Register', 'VirtualMachine.Inventory.Delete', 'VirtualMachine.Inventory.Unregister', 'VirtualMachine.Provisioning.DiskRandomAccess', 'VirtualMachine.Provisioning.DiskRandomRead', 'VirtualMachine.Provisioning.GetVmFiles', 'VirtualMachine.Provisioning.MarkAsTemplate', 'VirtualMachine.State.CreateSnapshot', 'VirtualMachine.State.RevertToSnapshot', 'VirtualMachine.State.RemoveSnapshot')</pre>
Network	<ul style="list-style-type: none"> Assign network 	
Resource	<ul style="list-style-type: none"> Assign virtual machine to resource pool Migrate powered off virtual machine Migrate powered on virtual machine 	
Sessions	<ul style="list-style-type: none"> Validate session 	
SPBM policy restore	<ul style="list-style-type: none"> Profile-driven storage view 	
vApp	<ul style="list-style-type: none"> Export Import vApp application configuration 	
Virtual Machine		
Change Configuration	<ul style="list-style-type: none"> Acquire disk lease Add existing disk Add new disk Add or remove device Advanced configuration Change CPU count Change Memory Change Settings Change Swapfile placement Change resource Configure Host USB device Configure Raw device Configure managedby Extend virtual disk Modify device settings Reload from path Remove disk Rename Reset guest information Set annotation Toggle disk change tracking Upgrade virtual machine compatibility 	
Edit Inventory	<ul style="list-style-type: none"> Create new Register Remove Unregister 	
Guest operations	<ul style="list-style-type: none"> Guest operation modifications Guest operation program execution Guest operation queries 	
Interaction	<ul style="list-style-type: none"> Configure CD media Connect devices Console interaction 	

New-VIRole -Name 'PowerProtect'

Table 50. Minimum required cloud-based vCenter user account privileges (continued)

Setting	vCenter 6.0 and later required privileges	PowerCLI equivalent required privileges
	<ul style="list-style-type: none"> Guest operating system management by VIX API Install VMware Tools Power off Power on Reset 	<pre>-Privilege (Get-VIPrivilege -Id \$privileges)</pre>
Provisioning	<ul style="list-style-type: none"> Allow disk access Allow read-only disk access Allow virtual machine download Mark as template 	
Snapshot Management	<ul style="list-style-type: none"> Create snapshot Remove snapshot Revert to snapshot 	

Add a VM Direct Engine

Perform the following steps in the **Protection Engines** window of the PowerProtect Data Manager UI to deploy an external VM Direct Engine, also referred to as a VM proxy. The VM Direct Engine facilitates data movement for virtual-machine protection policies.

Prerequisites


Review the sections [Requirements for an external VM Direct Engine](#) on page 66 and [Transport mode considerations](#) on page 252.

If applicable, complete all of the virtual network configuration tasks before you assign any virtual networks.


About this task

The PowerProtect Data Manager software comes 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 you deploy external proxies by adding a VM Direct Engine for the following reasons:

- An external VM Direct Engine for VM proxy backup and recovery can provide improved performance and reduce network bandwidth utilization by using source-side deduplication.
- The embedded VM Direct engine has limited capacity for backup streams.
- The embedded VM Direct engine is not supported for VMC-on-AWS, AVS-on-Azure, or GCVE-on-GCP operations.

 **NOTE:** Cloud-based deployments of PowerProtect Data Manager do not support the configuration of data-traffic routing or VLANs. Skip the **Networks Configuration** page.

Steps

1. From the left navigation pane, select **Infrastructure > Protection Engines**.
The **Protection Engines** window appears.
2. In the **VM Direct Engines** pane of the **Protection Engines** window, click **Add**.
The **Add Protection Engine** wizard displays.
3. On the **Protection Engine Configuration** page, complete the required fields, which are marked with an asterisk.
 - **Hostname, Gateway, IP Address, Netmask, and Primary DNS**—Note that only IPv4 addresses are supported.
 - **vCenter to Deploy**—If you have added multiple vCenter Server instances, select the vCenter on which to deploy the protection engine.
 **NOTE:** Ensure that you do not select the internal vCenter Server.
 - **ESX Host/Cluster**—Select on which cluster or ESXi host you want to deploy the protection engine.
 - **Network**—Displays all the networks that are available under the selected ESXi Host/Cluster. For virtual networks (VLANs), this network carries management traffic.

- **Data Store**—Displays all datastores that are accessible to the selected ESXi Host/Cluster based on ranking (whether the datastores are shared or local), 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 protection engine resides, or leave the default selection of **<automatic>** to allow PowerProtect Data Manager to determine the best location to host the protection engine.

- **Transport Mode**—Select **Hot Add**.
- **Supported Protection Type**—Select whether this protection engine is intended for **Virtual Machine**, **Kubernetes** Tanzu guest cluster, or **NAS** asset protection.

4. Click **Next**.
5. Click **Next** to skip the **Networks Configuration** page..
6. On the **Summary** page, review the information and then click **Finish**.

The protection engine is added to the **VM Direct Engines** pane. An additional column indicates the engine purpose. Note that it can take several minutes to register the new protection engine in PowerProtect Data Manager. The protection engine also appears in the **vSphere Client**.

Results

When an external VM Direct Engine is deployed and registered, PowerProtect Data Manager uses this engine instead of the embedded VM Direct engine for any data protection operations that involve virtual machine protection policies. If every external VM Direct Engine is unavailable, PowerProtect Data Manager uses the embedded VM Direct engine as a fallback to perform limited scale backups and restores. If you do not want to use the external VM Direct Engine, you can disable this engine.

[Additional VM Direct actions](#) on page 68 provides more information.

NOTE: The external VM Direct Engine is always required for VMC-on-AWS, AVS-on-Azure, and GCVE-on-GCP operations. If no external VM Direct Engine is available for these solutions, data protection operations fail.

Next steps

If the protection engine 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, delete the failed protection engine and then add the protection engine in the **Protection Engines** window.

When configuring the VM Direct Engine in a VMC-on-AWS, AVS-on-Azure, or GCVE-on-GCP environment, if you deploy the VM Direct Engine to the root of the cluster instead of inside the Compute-ResourcePool, you must move the VM Direct Engine inside the Compute-ResourcePool.

Unsupported operations

PowerProtect Data Manager image backup and restore in GCVE on GCP does not currently support the following operations:

- PowerProtect Search functionality
- A VM Direct appliance that is configured with dual-stack or IPv6
- Application-consistent data protection for Microsoft SQL with the VM Direct appliance
- VM Backup and Recovery HTML5 plug-in functionality for vSphere
- Image-based backups and restores that use NBD or the NBDSSL transport mode
- Image-based backups and restores when a datacenter is placed inside a folder in the SDDC
- File-level recoveries of an image-based backup
- Instant-access restores of an image-based backup
- Emergency restores of an image-based restore directly to an ESXi host, bypassing the vCenter server
- Backup and restore operations with anything other than the **CloudOwner** role or a customized role that has all of the privileges listed in [Specify the required privileges for a dedicated cloud-based vCenter user account](#) on page 193

NOTE: If protecting virtual-machine assets with a PowerProtect Data Manager machine image deployed to GCP, Cloud Disaster Recovery (CDR), Search Clusters, Microsoft Exchange, and block-based backups (BBB) with the File System agent (FSA) are also unsupported.

Performing Updates

Topics:

- [Managing update packages](#)
- [Updating the version of PowerProtect Data Manager](#)
- [Update PowerProtect Data Manager from version 19.8 to version 19.9](#)
- [Update PowerProtect Data Manager from version 19.7 to version 19.9](#)
- [Update PowerProtect Data Manager from versions 19.3–19.6 to version 19.9](#)

Managing update packages

You manage update packages from the **Software Update** window.

The **Software Update** window allows you to perform the following operations:

- Automatically or manually check for an update package
- Download an update package
- Upload an update package
- Delete an update package
- Perform a precheck on an update package
- Install an update package

Only the Administrator role can manage and perform updates.



Automatically check for an update package

You can configure PowerProtect Data Manager to automatically check for a new update package once a day. If a new update package is available, you can either be alerted or have it automatically downloaded.

Prerequisites

SupportAssist must be enabled. For more information, see [Configuring SupportAssist for PowerProtect Data Manager](#) on page 158 and [Enable or disable SupportAssist](#) on page 161.

Steps

1. Log in to the PowerProtect Data Manager user interface as a user with the Administrator role.
2. Click , and then select **Software Update**.
3. In the **Software Update** window, click **Check for Updates**.
4. In the **Software Update > Check for Updates** pane, click .
5. In the **Configure Updates** window, choose what happens if a new package update is available.
 - To only be notified of the package update, select **Check and notify**.
 - To automatically download the package update, select **Check and automatically download**.
6. Click **Save**.

Troubleshooting automatic downloads

Even if PowerProtect Data Manager has been configured to automatically download any new update package, there are a couple of conditions that disable this feature.

The following table describes the common issues with automatic downloads and how to resolve them.

Table 51. Common issues with automatic downloads

Issue	Reason	Resolution
Automatic downloads are disabled.	There is already an update package ready to install and displayed in the Software Update > Install Update pane.	Delete or install the existing update package.
The wrong update package was automatically downloaded.	If there is more than one new package update available, the most recent one is automatically downloaded.	Delete the update package that was automatically downloaded, and then manually download and install the desired update package.


Manually check for an update package

You can use the PowerProtect Data Manager user interface to manually check for a new update package.

Prerequisites

SupportAssist must be enabled. For more information, see [Configuring SupportAssist for PowerProtect Data Manager](#) on page 158 and [Enable or disable SupportAssist](#) on page 161.

Steps

1. Log in to the PowerProtect Data Manager user interface as a user with the Administrator role.
2. Click , and then select **Software Update**.
3. In the **Software Update** window, click **Check for Updates**.
4. In the **Software Update > Check for Updates** pane, click **Check Now**.

Results

All available update packages are displayed in the **Software Update > Check for Updates** pane. If there is more than one update package available, more information about each can be seen.


Download an update package


If an update package is available, you can download it to PowerProtect Data Manager for later installation.

About this task

The **Software Update > Install Update** pane displays any update package ready to install. If an update package is already ready to install, it will be overwritten by this procedure.

Steps

1. Log in to the PowerProtect Data Manager user interface as a user with the Administrator role.
2. Click , and then select **Software Update**.
3. In the **Software Update** window, click **Check for Updates**.
All available update packages are displayed. If there is more than one update package available, more information about each can be seen.
4. From the **Software Update > Check for Updates** pane, select the update package to download, and then click **Download**.

 **NOTE:** If an update package is already ready to install, you will be asked to confirm if you want to overwrite it.

Results

The update package is downloaded to PowerProtect Data Manager and displayed as ready to install in the **Software Update > Install Update** pane.


Upload an update package


If SupportAssist is not enabled, you do not want to enable it, and you know there is a new update package available that you want to install, then you need to manually upload it to PowerProtect Data Manager.

About this task

The **Software Update > Install Update** pane displays any update package ready to install. If an update package is already ready to install, it will be overwritten by this procedure.

Steps

1. Download the update package from [Dell EMC Support Downloads and Drivers](#).
2. Log in to the PowerProtect Data Manager user interface as a user with the Administrator role.
3. Click , and then select **Software Update**.
4. In the **Software Update** window, click **Install Update**.
5. From the **Software Update > Install Update** pane, click **Upload Package**, and select the upload package to upload.

 **NOTE:** If an update package is already ready to install, you will be asked to confirm if you want to overwrite it.


Results

The update package is uploaded to PowerProtect Data Manager and displayed as ready to install in the **Software Update > Install Update** pane.

Delete an update package

If you decide you are not going to install an update package that is ready to install, you can delete it.

Steps

1. Log in to the PowerProtect Data Manager user interface as a user with the Administrator role.
2. Click , and then select **Software Update**.
3. In the **Software Update** window, click **Install Update**.
The **Software Update > Install Update** pane displays the update package ready to install.
4. From the **Software Update > Install Update** pane, click **Delete**.

Results


The **Software Update > Install Update** pane is empty, and the update package is no longer ready to install.

Perform a precheck on an update package

After an update package has been downloaded or uploaded, you can perform a precheck on it to verify it is compatible with the current configuration of PowerProtect Data Manager.

Steps

1. Log in to the PowerProtect Data Manager user interface as a user with the Administrator role.

2. Click , and then select **Software Update**.
3. In the **Software Update** window, click **Install Update**.
The **Software Update > Install Update** pane displays the update package ready to install.
4. From the **Software Update > Install Update** pane, click **Precheck**.

 **NOTE:** You can navigate away from the **Software Update > Install Update** pane while the precheck is running or even exit the PowerProtect Data Manager interface without interrupting the precheck.


Results

The results of the precheck are displayed in the **Software Update > Install Update** pane.

Install an update package

After an update package has been downloaded or uploaded, you can install it to PowerProtect Data Manager.

Steps

1. Log in to the PowerProtect Data Manager user interface as a user with the Administrator role.
2. Click , and then select **Software Update**.
3. In the **Software Update** window, click **Install Update**.
The **Software Update > Install Update** pane displays the update package ready to install.
4. From the **Software Update > Install Update** pane, click **Install**.

Results

If the installation succeeds, the update package is removed from the **Software Update > Install Update** pane. However, you can click the **History** tab from **Software Update > Install Update** pane to see a history of all successful updates.

If the installation fails, the update package remains in the **Software Update > Install Update** pane, along with details of the failure.

Updating the version of PowerProtect Data Manager

This section provides instructions for updating PowerProtect Data Manager from an older version to the most recent version.

If you are updating PowerProtect Data Manager from version 19.8 to version 19.9, follow the steps in [Update PowerProtect Data Manager from version 19.8 to version 19.9](#) on page 214.

If you are updating PowerProtect Data Manager from version 19.7 to version 19.9, follow the steps in [Update PowerProtect Data Manager from version 19.7 to version 19.9](#) on page 216.

If you are updating PowerProtect Data Manager from versions 19.3–19.6 to version 19.9, follow the steps in [Update PowerProtect Data Manager from versions 19.3–19.6 to version 19.9](#) on page 218.

Migrating to SupportAssist


SupportAssist provides automated support capabilities for PowerProtect Data Manager systems. SupportAssist replaces Secure Remote Services (SRS).

If you have configured SRS previously, the PowerProtect Data Manager system automatically migrates SRS to SupportAssist when you update PowerProtect Data Manager.

If you do not have SRS configured, you can configure SupportAssist directly. [Connect to the SupportAssist Enterprise](#) on page 159 provides instructions for configuring SupportAssist.

Updating DD or DDVE

If you are updating DD or DDVE software at the same time as PowerProtect Data Manager, ensure that the following sequence of events is followed:

1. Disable all protection policies that use the affected DD or DDVE storage systems.
2. If there are any running jobs that were started by the protection policies, wait for them to complete.
 **NOTE:** Any scheduled replication, cloud tier, or extended replication jobs will continue to run, and might fail during the update.
3. Update the DD or DDVE software.
4. Enable all protection policies that were disabled.

Updating from version 19.8 or earlier in a Kubernetes environment

If you are updating from version 19.8 or earlier and have Kubernetes configured, see the *PowerProtect Data Manager for Kubernetes User Guide* for additional Kubernetes-specific considerations.

 **CAUTION:** If you do not follow a Kubernetes-specific update procedure, PowerProtect Data Manager might fail to function properly.

Update PowerProtect Data Manager from version 19.8 to version 19.9

Use this procedure to update PowerProtect Data Manager from 19.8 to version 19.9 or to apply critical updates.

Prerequisites


- Download the update package from [Dell EMC Support Downloads and Drivers](#).
- Only the Administrator role can perform updates.
- Check for running tasks and cancel them or allow them to complete.
- For on-premise installations, take a manual snapshot of the VM in vCenter, or enable automatic snapshots. Ensure that the vCenter hosting PowerProtect Data Manager is added as an asset source, and that the user account associated with the vCenter host has the following permissions:

Setting	vCenter 6.0 and later required privileges	PowerCLI equivalent required privileges
Global	<ul style="list-style-type: none">○ Manage custom attributes○ Set custom attributes	<ul style="list-style-type: none">○ Global.ManageCustomFields○ Global.SetCustomField
Virtual Machine Snapshot Management	<ul style="list-style-type: none">○ Create snapshot○ Revert to snapshot○ Remove snapshot○ Rename snapshot	<ul style="list-style-type: none">○ VirtualMachine.State.CreateSnapshot○ VirtualMachine.State.RevertToSnapshot○ VirtualMachine.State.RemoveSnapshot○ VirtualMachine.State.RenameSnapshot

- For cloud-based installations, perform a backup of the AWS instance or Azure VM. The AWS and Azure documentation provides instructions.


About this task

You can update the system by manually downloading update packages or by connecting to a Secure Remote Services (SRS) gateway. When PowerProtect Data Manager is licensed and you have registered the SRS gateway host with PowerProtect Data Manager, you can update using SRS. When an update package is available, the packages are uploaded to the SRS gateway. The appliance checks the SRS gateway once a day for available update packages or you can manually check [Dell EMC Support Downloads and Drivers](#) for update packages.

 **NOTE:** If SRS is configured and a critical update is available in the SRS gateway, a notification appears in the UI. You can also download available critical updates that appear in the **Support Site** section of the **Upgrade** page.

An update package can update 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
- Kubernetes support
- PowerProtect Search software
- Remote Cloud Disaster Recovery Server

 **NOTE:** If you have your own SSL certificate that you wish to continue using, the *PowerProtect Data Manager Security Configuration Guide* provides more information.

In PowerProtect Data Manager, the update process automatically stops and removes most running jobs and puts the system into maintenance mode. If server Disaster Recovery is enabled, the system performs a Server DR backup. If automatic snapshots are configured, the update process creates a VM snapshot of the system. If the update fails or is aborted, the system uses the snapshot to roll back to the previous state. Once the system is rolled back or update successfully, the snapshot is automatically deleted.


You can check if the PowerProtect Data Manager system is ready to update by running a manual precheck. [Run a manual precheck](#) on page 221 provides more information.

Steps

1. Log in to the PowerProtect Data Manager user interface as a user with the Administrator role.

2. Click , and then select **Software Update**.

The **Software Update** window lists any packages that have already been downloaded, in descending date order. If you have registered SRS, the latest available PowerProtect Data Manager update package appears in the **Support Site** section of the window. For any package, you can click the down arrow next to the package name to view details about the contents.

 **NOTE:** When the PowerProtect Data Manager system is configured to automatically check for updates, the download of any newly discovered update package cannot proceed if there is already an update package in local storage.

To download the latest available update package, remove the existing package.

3. If you have registered SRS, in the row for the update package, click **Download**.


If you enabled PowerProtect Data Manager to automatically download update packages in **System Settings > Support > Secure Remote Services**, PowerProtect Data Manager downloads the update package automatically.

When the download is complete, the update package appears in the **Packages** section.

4. If you have not registered SRS and you are using the manual package download method:
 - a. Click **Upload Package**.
 - b. Browse to the path that contains the update package, select the package, and then click **Open**.
 - c. Wait until the package has fully downloaded, and then click **OK**.

5. When the update package status indicates **Available**, click  to start the update wizard.


6. The update wizard consists of 3 stages. Click **Next** at the first two stages, and **Finish** at the last stage.

 **NOTE:** You can also click **Back** or **Cancel** at any stage.

- a. **Precheck.** The update manager runs a precheck.


- If a critical issue is found, the update is cancelled. Fix any issues and run the precheck to ensure that the issue is fixed.
- If non-critical issues are found, Dell EMC recommends that you fix any issues and run the precheck before proceeding with the update.

- b. **Security.** Review the details of the security certificate.

 **NOTE:** You will not see this stage of the wizard if you accepted the security certificate during a previous update.

- c. **Summary.** Review the details of the update.

The update begins. The browser is redirected to the Upgrade Manager UI on port 14443. This action enables you to monitor update progress while the PowerProtect Data Manager components are shutdown for the update.


 **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 update, if necessary.

When the update completes successfully, the browser is redirected back to the main PowerProtect Data Manager UI login page.

Results

The **Upgrade** page indicates the status of the update.

- If the update fails, but PowerProtect Data Manager is still running:
 1. Wait for the Upgrade Manager to finish processing.
 2. Click **Return to Dashboard** and log in to view the issue.
 3. Click , and then select **Software Update**.
 4. Expand the package that was installed to view the issue that caused the failure:
 - If one or more core update fail, the status of the update package indicates **Failed**.
 - If all core updates complete, but a VM Direct Engine, the Search Cluster, are another non-core component is still processing, the update package status indicates **Installed (Core)**.
 - If all core updates complete, but a VM Direct Engine, the Search Cluster, or another non-core component fails to update, the update package status indicates **Installed With Errors**.
 5. Fix the issue that caused the failure and run the precheck again.

If the precheck is successful, the package status changes to **Available** and the update can be retried.

6. Retry the update.

When you retry the update, PowerProtect Data Manager only retries the components that failed.

- If the update fails and PowerProtect Data Manager is not running:
 1. Click **Export Logs** to download the log files for troubleshooting.
 2. If an automatic snapshot was taken, click **Rollback to snapshot** to restore the core PowerProtect Data Manager system to its state before the update.
 3. Review the log files to determine the cause of the failure.
 - If you can resolve the issues manually, try the update again.
 - If you cannot resolve the issues, contact [Dell EMC Support](#).

Update PowerProtect Data Manager from version 19.7 to version 19.9

Use this procedure to update PowerProtect Data Manager from 19.7 to version 19.9 or to apply critical updates.

Prerequisites

- Download the update package from [Dell EMC Support Downloads and Drivers](#).
- Only the Administrator role can perform updates.
- Check for running tasks and cancel them or allow them to complete.
- For on-premise installations, take a manual snapshot of the VM in vCenter, or enable automatic snapshots. Ensure that the vCenter hosting PowerProtect Data Manager is added as an asset source, and that the user account associated with the vCenter host has the following permissions:

Setting	vCenter 6.0 and later required privileges	PowerCLI equivalent required privileges
Global	<ul style="list-style-type: none">◦ Manage custom attributes◦ Set custom attributes	<ul style="list-style-type: none">◦ Global.ManageCustomFields◦ Global.SetCustomField
Virtual Machine Snapshot Management	<ul style="list-style-type: none">◦ Create snapshot◦ Revert to snapshot◦ Remove snapshot◦ Rename snapshot	<ul style="list-style-type: none">◦ VirtualMachine.State.CreateSnapshot◦ VirtualMachine.State.RevertToSnapshot◦ VirtualMachine.State.RemoveSnapshot◦ VirtualMachine.State.RenameSnapshot

- For cloud-based installations, perform a backup of the AWS instance or Azure VM. The AWS and Azure documentation provides instructions.

About this task

You can update the system by manually downloading update packages or by connecting to a Secure Remote Services (SRS) gateway. When PowerProtect Data Manager is licensed and you have registered the SRS gateway host with PowerProtect Data Manager, you can update using SRS. When an update package is available, the packages are uploaded to the SRS gateway. The appliance checks the SRS gateway once a day for available update packages or you can manually check [Dell EMC Support Downloads and Drivers](#) for update packages.

NOTE: If SRS is configured and a critical update is available in the SRS gateway, a notification appears in the UI. You can also download available critical updates that appear in the **Support Site** section of the **Upgrade** page.

An update package can update 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
- Kubernetes support
- PowerProtect Search software
- Remote Cloud Disaster Recovery Server

NOTE: If you have your own SSL certificate that you wish to continue using, the *PowerProtect Data Manager Security Configuration Guide* provides more information.

In PowerProtect Data Manager, the update process automatically stops and removes most running jobs and puts the system into maintenance mode. If server Disaster Recovery is enabled, the system performs a Server DR backup. If automatic snapshots are configured, the update process creates a VM snapshot of the system. If the update fails or is aborted, the system uses the snapshot to roll back to the previous state. Once the system is rolled back or update successfully, the snapshot is automatically deleted.

You can check if the PowerProtect Data Manager system is ready to update by running a manual precheck. [Run a manual precheck](#) on page 221 provides more information.

Steps

1. Log in to the PowerProtect Data Manager user interface as a user with the Administrator role.

2. Click , and then select **Software Update**.

The **Software Update** window lists any packages that have already been downloaded, in descending date order. If you have registered SRS, the latest available PowerProtect Data Manager update package appears in the **Support Site** section of the window. For any package, you can click the down arrow next to the package name to view details about the contents.

NOTE: When the PowerProtect Data Manager system is configured to automatically check for updates, the download of any newly discovered update package cannot proceed if there is already an update package in local storage.

To download the latest available update package, remove the existing package.

3. If you have registered SRS, in the row for the update package, click **Download**.

If you enabled PowerProtect Data Manager to automatically download update packages in **System Settings > Support > Secure Remote Services**, PowerProtect Data Manager downloads the update package automatically.

When the download is complete, the update package appears in the **Packages** section.

4. If you have not registered SRS and you are using the manual package download method:

- a. Click **Upload Package**.
- b. Browse to the path that contains the update package, select the package, and then click **Open**.
- c. Wait until the package has fully downloaded, and then click **OK**.

5. When the update package status indicates **Available**, click  to start the update wizard.

6. The update wizard consists of 3 stages. Click **Next** at the first two stages, and **Finish** at the last stage.

NOTE: You can also click **Back** or **Cancel** at any stage.

a. **Precheck.** The update manager runs a precheck.

- If a critical issue is found, the update is cancelled. Fix any issues and run the precheck to ensure that the issue is fixed.


- If non-critical issues are found, Dell EMC recommends that you fix any issues and run the precheck before proceeding with the update.

b. **Authentication.** Enter the lockbox passphrase if required.

Review the section [Lockbox passphrase required when updating from some versions](#) on page 221.

c. **Summary.** Review the details of the update.

The update begins. The browser is redirected to the Upgrade Manager UI on port 14443. This action enables you to monitor update progress while the PowerProtect Data Manager components are shutdown for the update.


 **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 update, if necessary.

When the update completes successfully, the browser is redirected back to the main PowerProtect Data Manager UI login page.

Results


The **Upgrade** page indicates the status of the update.

- If the update fails, but PowerProtect Data Manager is still running:
 1. Wait for the Upgrade Manager to finish processing.
 2. Click **Return to Dashboard** and log in to view the issue.
 3. Click , and then select **Software Update**.
 4. Expand the package that was installed to view the issue that caused the failure:
 - If one or more core update fail, the status of the update package indicates **Failed**.
 - If all core updates complete, but a VM Direct Engine, the Search Cluster, are another non-core component is still processing, the update package status indicates **Installed (Core)**.
 - If all core updates complete, but a VM Direct Engine, the Search Cluster, or another non-core component fails to update, the update package status indicates **Installed With Errors**.
 5. Fix the issue that caused the failure and run the precheck again.

If the precheck is successful, the package status changes to **Available** and the update can be retried.

6. Retry the update.

When you retry the update, PowerProtect Data Manager only retries the components that failed.

- If the update fails and PowerProtect Data Manager is not running:
 1. Click **Export Logs** to download the log files for troubleshooting.
 2. If an automatic snapshot was taken, click **Rollback to snapshot** to restore the core PowerProtect Data Manager system to its state before the update.
 3. On the **Upgrade** page, click  to delete the failed update package.
 4. Review the log files to determine the cause of the failure.
 - If you can resolve the issues manually, try the update again.
 - If you cannot resolve the issues, contact [Dell EMC Support](#).

Update PowerProtect Data Manager from versions 19.3–19.6 to version 19.9

Use this procedure to update PowerProtect Data Manager from versions 19.3 through 19.6 to version 19.9 or to apply critical updates.

Prerequisites

- Download the update package from [Dell EMC Support Downloads and Drivers](#).
- Only the Administrator role can perform updates.
- Check for running tasks and cancel them or allow them to complete.
- For on-premise installations, take a manual snapshot of the VM in vCenter, or enable automatic snapshots. Ensure that the vCenter hosting PowerProtect Data Manager is added as an asset source, and that the user account associated with the vCenter host has the following permissions:

Setting	vCenter 6.0 and later required privileges	PowerCLI equivalent required privileges
Global	<ul style="list-style-type: none"> Manage custom attributes Set custom attributes 	<ul style="list-style-type: none"> Global.ManageCustomFields Global.SetCustomField
Virtual Machine Snapshot Management	<ul style="list-style-type: none"> Create snapshot Revert to snapshot Remove snapshot Rename snapshot 	<ul style="list-style-type: none"> VirtualMachine.State.CreateSnapshot VirtualMachine.State.RevertToSnapshot VirtualMachine.State.RemoveSnapshot VirtualMachine.State.RenameSnapshot

- For cloud-based installations, perform a backup of the AWS instance or Azure VM. The AWS and Azure documentation provides instructions.
- If you are updating from version 19.3, ensure that you run an ad hoc DR backup operation to back up the Search Service, which is not included in the automatic DR backup that runs before the update.

About this task

You can update the system by manually downloading update packages or by connecting to a Secure Remote Services (SRS) gateway. When PowerProtect Data Manager is licensed and you have registered the SRS gateway host with PowerProtect Data Manager, you can update using SRS. When an update package is available, the packages are uploaded to the SRS gateway. The appliance checks the SRS gateway once a day for available update packages or you can manually check for update packages.

NOTE: If SRS is configured and a critical update is available in the SRS gateway, a notification appears in the UI. You can also download available critical updates that appear in the **Support Site** section of the **Software Upgrade** window.

An update package can update one or more of the following:

- The PowerProtect Data Manager software, including application agent installers stored on the PowerProtect Data Manager virtual machine
- External VM Direct appliance
- Kubernetes support
- PowerProtect Search software
- Remote Cloud Disaster Recovery Server

NOTE: If you have your own SSL certificate that you wish to continue using, the *PowerProtect Data Manager Security Configuration Guide* provides more information.


In PowerProtect Data Manager, the update process automatically stops most running jobs and puts the system into maintenance mode. If server Disaster Recovery is enabled, the system performs a Server DR backup. If automatic snapshots are configured, the update process creates a virtual machine snapshot of the system. If the update fails or is aborted, the system uses the snapshot to roll back to the previous state. Once the system is rolled back or update successfully, the snapshot is automatically deleted.

In PowerProtect Data Manager 19.5 and later, you can check if the PowerProtect Data Manager system is ready to update by running a manual precheck. [Run a manual precheck](#) on page 221 provides more information.

NOTE: When you update PowerProtect Data Manager, you are accepting the terms of the latest product EULA. If AutoSupport is enabled, you are also accepting the latest Telemetry Software Terms. It is recommended that you review the Telemetry Software Terms and EULA terms before continuing with the update.

After you upload the update package, the latest EULA (in both text and PDF format) and the Telemetry Software Terms (in PDF format) are available in the `/data01/brs/update/eulas` folder.

Steps

- Log in to the PowerProtect Data Manager user interface as a user with the Administrator role.
- Click , and then select **Upgrade**.

The window lists any packages that have already been downloaded, in descending date order. If you have registered SRS, the latest available PowerProtect Data Manager update package appears in the **Support Site** section of the window. For any package, you can click the down arrow next to the package name to view details about the contents.

NOTE: When the PowerProtect Data Manager system is configured to automatically check for update, the download of any newly discovered update package cannot proceed if there is already an update package in local storage.


To download the latest available update package, remove the existing package.


3. If you have registered SRS, in the row for the update package, click **Download**.

If you enabled PowerProtect Data Manager to automatically download update packages in **System Settings > Support > Secure Remote Services**, PowerProtect Data Manager downloads the update package automatically.

When the download is complete, the update package appears in the **Packages** section.

4. If you have not registered SRS and you are using the manual package download method:
 - a. Click **Upload Package**.
 - b. Browse to the path that contains the update package, select the package, and then click **Open**.
 - c. Wait until the package has fully downloaded, and then click **OK**.

5. When the update package status indicates **Available**, click  to start the update.


 **NOTE:** In PowerProtect Data Manager versions that are earlier than 19.5, click **Perform Upgrade**.

The **Software Upgrade** wizard appears.

6. On the **Precheck** page, the software update manager runs a precheck:
 - If a critical issue is found, the update is cancelled and the **Next** button is disabled. Fix any issues and then run the precheck again to ensure that the issue is fixed. When the precheck completes successfully, click **Next**.
 - If non-critical issues are found, you can click **Next** to proceed with the update, but Dell EMC recommends that you fix any issues and then run the precheck again before proceeding with the update.
 - If the precheck completes successfully with no issues, click **Next**.
7. On the **Security** page:
 - a. Enter the lockbox passphrase, if required. For example, if updating from PowerProtect Data Manager 19.7 to version 19.9, the lockbox passphrase is required if you have not previously accepted the certificate of the update package.
Review the section [Lockbox passphrase required when updating from some versions](#) on page 221 to determine if the version you are update from requires you to specify the lockbox passphrase.
 - b. Click **Next**.

8. On the **Summary** page, review the update package and certificate information, and then click **Finish** to proceed.

The update begins. The browser is redirected to the **Upgrade Manager** UI on port 14443. This action enables you to monitor update progress while the PowerProtect Data Manager components are shut down for the update.


 **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 update, if necessary.


When the update completes successfully, the browser is redirected back to the main PowerProtect Data Manager UI login page.

Results

The **Software Upgrade** window indicates the status of the update.

- If the update fails, but PowerProtect Data Manager is still running:
 1. Wait for the Upgrade Manager to finish processing.
 2. Click **Return to Dashboard** and log in to view the issue.
 3. Click , and then select **Upgrade**.
 4. Expand the package that was installed to view the issue that caused the failure:
 - If one or more core update fail, the status of the update package indicates **Failed**.
 - If all core update complete, but one or more non-core components, such as vProxies and Search Cluster are still processing, the update package status indicates **Installed (Core)**.
 - If all core updates complete, but one or more non-core components, such as vProxies and Search Cluster fail to update, the update package status indicates **Installed With Errors**.
 5. Fix the issue that caused the failure and run the precheck again.
If the precheck is successful, the package status changes to **Available** and the update can be retried.
 6. Retry the update.

When you retry the update, PowerProtect Data Manager only retries the components that failed.

- If the update fails and PowerProtect Data Manager is not running:
 1. Click **Export Logs** to download the log files for troubleshooting.
 2. If an automatic snapshot was taken, click **Rollback to snapshot** to restore the core PowerProtect Data Manager system to its state before the update.
 3. On the **Upgrade** page, click  to delete the failed update package.
 4. Review the log files to determine the cause of the failure.
 - If you can resolve the issues manually, try the update again.
 - If you cannot resolve the issues, contact [Dell EMC Support](#).

Run a manual precheck


For PowerProtect Data Manager versions 19.5 and 19.6, you can run a manual precheck to check if the PowerProtect Data Manager system is ready to update or to verify that any issues that caused a previous precheck to fail are now resolved.

About this task


To run a manual precheck, complete the following steps:

Steps

1. Log in to the PowerProtect Data Manager user interface as a user with the Administrator role.

2. Click , and then select **Upgrade**.

3. To upload an update package:

 **NOTE:** You can skip this step if you have already uploaded the update package.

- a. Click **Upload Package**, browse to the path that contains the update package, select the package, and then click **Open**.
- b. Wait until the package status is Available, and then click **OK**.

Click the down arrow next to the package name to view details about the contents.

4. To run the precheck, click  in the **Actions** column.

When the precheck is complete, a dialog box lists any areas that require attention, such as indication that the update is disruptive or requires a reboot. The dialog box also includes warnings about running tasks or active sessions that should be addressed before the update. Click the links that are provided to go to the management page for the active events, where you can cancel them or allow them to complete before continuing.

The dialog box also indicates if any application agents managed by PowerProtect Data Manager are not compatible with the latest version of the PowerProtect Data Manager system. Manually update the application agents to the latest version before you update the PowerProtect Data Manager system.

If critical issues are found, the precheck fails and the update cannot proceed. If non-critical issues are found, Dell EMC recommends that you fix any issues before proceeding with the update.

Lockbox passphrase required when updating from some versions

In some circumstances, the lockbox passphrase is required to proceed with the PowerProtect Data Manager update.


The following table identifies whether the lockbox passphrase is required when updating to version 19.9, depending on the PowerProtect Data Manager version you are updating from.

Table 52. Lockbox passphrase requirements

Updating from version	Lockbox passphrase required?
19.3	See note.
19.4	No
19.5	No
19.6	No

Table 52. Lockbox passphrase requirements (continued)

Updating from version	Lockbox passphrase required?
19.7	Yes, if you have not previously updated the system and accepted the update-package certificate. Otherwise, no.
19.8	No

 **NOTE:** Before automatic lockbox management, updates from version 19.3 required you to provide the lockbox passphrase. Because PowerProtect Data Manager now manages this passphrase, you can type any text in the passphrase field to bypass this step. PowerProtect Data Manager overrides this text with the decrypted lockbox passphrase.

Configuring and Managing the PowerProtect Agent Service

Topics:

- [About the PowerProtect agent service](#)
- [Start, stop, or obtain the status of the PowerProtect agent service](#)
- [Register the PowerProtect agent service to a different server address](#)
- [Recovering the PowerProtect agent service from a disaster](#)

About the PowerProtect agent service

The PowerProtect agent service is a REST API based service that is installed by the application agent on the application host. The agent service provides services and APIs for discovery, protection, restore, instant access, and other related operations. The PowerProtect Data Manager uses the agent service to provide integrated data protection for the application assets.

This section uses `<agent_service_installation_location>` to represent the PowerProtect agent service installation directory. By default, the agent service installation location is `C:\Program Files\DPSAPPS\AgentService` on Windows and `/opt/dpsapps/agentsvc` on Linux. All files that are referenced in this section are the relative paths to the agent service installation location.

The PowerProtect agent service performs the following operations:

- **Addon detection**—An addon integrates the application agent into the agent service. The agent service automatically detects the addons on the system for each application asset type and notifies the PowerProtect Data Manager. While multiple addons can operate with different asset types, only one agent service runs on the application host. Specific asset types can coexist on the same application host.
- **Discovery**—The agent service discovers both stand-alone and clustered database servers (application systems), databases and file systems (assets), and their backup copies on the application agent host. After the initial discovery, when the agent service discovers any new application systems, assets, or copies, the agent service notifies the PowerProtect Data Manager.
- **Self-service configuration**—The agent service can configure the application agent for self-service operations by using information that is provided by the PowerProtect Data Manager. When you add an asset to a protection policy for self-service or centralized protection, or modify the protection policy, including changing the DD Boost credentials, the PowerProtect Data Manager automatically pushes the protection configuration to the agents.

NOTE: If you change the DD Boost credentials to include \ in the password, the protection policy configuration will not be pushed to the agents unless you also select the protection policy from the **Protection Policies** window, and then click **Set LockBox**.

- **Centralized backups**—The agent service performs the centralized backups as requested by the PowerProtect Data Manager.
 - **Centralized restores**—The agent service performs the centralized restores as requested by the PowerProtect Data Manager.
- NOTE:** In the current release, the centralized restores are only available for the File System agent, Microsoft SQL agent, and Storage Direct agent.
- **Backup deletion and catalog cleanup**—The PowerProtect Data Manager deletes the backup files directly from the protection storage when a backup expires or an explicit delete request is received and no dependent (incremental or log) backups exist. The PowerProtect Data Manager goes through the agent service to delete the catalog entries from the database vendor's catalog and the agent's local datastore.

NOTE: Deletion of any backup copies manually or through the command line is not recommended. PowerProtect Data Manager deletes all the expired copies as needed.

The agent service is started during the agent installation by the installer. The agent service runs in the background as a service and you do not interact with it directly.

The `config.yml` file contains the configuration information for the agent service, including several parameter settings that you can change within the file. The `config.yml` file is located in the `<agent_service_installation_location>` directory.

The agent service periodically starts subprocesses to perform the discovery jobs. You can see the type and frequency of these jobs in the `jobs:` section of the `config.yml` file. The job interval unit is minutes.

The agent service maintains a datastore in the `<agent_service_installation_location>/dbs/v1` directory, which contains information about the application system, assets, and backups discovered on the system. The size of the datastore files depends on the number of applications and copies on the host. The agent service periodically creates a backup of its datastore in the `<agent_service_installation_location>/dbs/v1/backups` directory, as used to recover the datastore if this datastore is lost.

NOTE: The size of each datastore backup is the same as the datastore itself. By default, a backup is created every hour. To save space on the file system, you can reduce this datastore backup frequency for large datastores. By default, the datastore backup is retained for one week. You can change the datastore backup frequency, retention period, and backup location in the `config.yml` file.

Start, stop, or obtain the status of the PowerProtect agent service

The PowerProtect agent service is started during the agent installation by the installer. If needed, you can use the appropriate procedure to start, stop, or obtain the status of the agent service.

On Linux, you can start, stop, or obtain the status of the agent service by running the `register.sh` script that is found in the `<agent_service_installation_location>` directory.

- To start the agent service:

```
# register.sh --start
Started agent service with PID - 1234
```

- To stop the agent service:

```
# register.sh --stop
Successfully stopped agent-service.
```

- To obtain the status when the agent service is running:

```
# register.sh --status
Agent-service is running with PID - 1234
```

- To obtain the status when the agent service is not running:

```
# register.sh --status
Agent-service is not running.
```


On Windows, you can start, stop, or obtain the status of the PowerProtect agent service from the Services Manager, similar to other Windows services. The name of the service in Services Manager is **PowerProtect Agent Service**.

Register the PowerProtect agent service to a different server address

The PowerProtect agent service is registered to a particular PowerProtect Data Manager server during the agent installation by the installer. If needed, you can register the agent service to a different PowerProtect Data Manager server address.

The agent service can only be registered to a single PowerProtect Data Manager server. When you register the agent service to a new server, the agent service will automatically unregister from the previous server address.

On Linux, you can register the agent service to a different server address by running the `register.sh` script that is found in the `<agent_service_installation_location>` directory.

 **NOTE:** The `register.sh` script stops the currently running agent service.

- The following command prompts for the new IP address or hostname:

```
# register.sh

Enter the PowerProtect Data Manager IP address or hostname: 10.0.0.1

Warning: Changing IP of PowerProtect Server from 192.168.0.1 to 10.0.0.1

Started agent service with PID - 1234
```

- The following command includes the new IP address on the command line:

```
# register.sh --ppdmServer=10.0.0.1

Warning: Changing IP of PowerProtect Server from 192.168.0.1 to 10.0.0.1

Started agent service with PID - 1234
```

On Windows, you can change the PowerProtect Data Manager server address by launching the agent installer and selecting the change option. Change the PowerProtect Data Manager service address from the **Configuration Install Options** page.

Recovering the PowerProtect agent service from a disaster

You can perform self-service restores of application assets by using a file system or application agent, regardless of the state of the agent service or PowerProtect Data Manager. The information in this section describes how to bring the agent service to an operational state to continue if a disaster occurs and the agent service datastore is lost.


The agent service periodically creates a backup of its datastore in the `<agent_service_installation_location>/dbs/v1/backups` repository. If all these backups are lost, the agent service can still start. The agent service discovers all the application systems, assets, and backup copies on the system again, and notifies PowerProtect Data Manager. Depending on when the failure occurred, the agent service might not be able to find older backup copies for some asset types. As a result, the centralized deletion operations might fail when cleaning up the database vendor catalog or removing older backups that are taken before the asset is added to PowerProtect Data Manager.

By default, the agent service backs up consistent copies of its datastore files to the local disk every hour and keeps the copies for 7 days. Each time the agent service backs up the contents of the datastore, it creates a subdirectory under the `<agent_service_installation_location>/dbs/v1/backups` repository. The subdirectories are named after the time the operation occurred, in the format `YYYY-MM-DD_HH-MM-SS_epochTime`.

By default, the datastore repository is on the local disk. To ensure that the agent service datastore and its local backups are not lost, it is recommended that you back up the datastore through file system backups. You can also change the datastore backup location to a different location that is not local to the system. To change the datastore backup location, update the values in the `config.yml` file.

Restore the PowerProtect Data Manager agent service datastore

Prerequisites

 **NOTE:** Ensure that the agent service is powered off. Do not start the agent service until disaster recovery is complete.

About this task

You can restore the datastore from the datastore backup repository. If the repository is no longer on the local disk, restore the datastore from file system backups first.

To restore the datastore from a backup in the datastore backup repository, complete the following steps:

Steps

1. Move the files in the `<agent_service_installation_location>/dbs/v1` directory to a location for safe keeping.



NOTE: Do not move or delete any `<agent_service_installation_location>/dbs/v1` subdirectories.

2. Select the most recent datastore backup.

The directories in the datastore backup repository are named after the time the backup was created.

3. Copy the contents of the datastore backup directory to the `<agent_service_installation_location>/dbs/v1` directory.

After the copy operation is complete, the `<agent_service_installation_location>/dbs/v1` directory should contain the following files:

- `copies.db`
- `objects.db`
- `resources.db`
- `sessions.db`

4. Start the agent service.

Backing Up and Recovering a vCenter Server

Topics:

- [Backing up and recovering a vCenter server](#)
- [vCenter deployments overview](#)
- [Protecting an embedded PSC](#)
- [Protecting external deployment models](#)
- [vCenter server restore workflow](#)
- [Platform Services Controller restore workflow](#)
- [Additional considerations](#)
- [Command reference](#)

Backing up and recovering a vCenter server

The following sections describe how to protect the vCenter server Appliance (VCSA) and the Platform Services Controllers (PSC). It is intended for virtual administrators who utilize the distributed model of the vCenter server and require protection of the complete vCenter server infrastructure.

vCenter deployments overview

You can protect vCenter 6.5 deployments with PowerProtect Data Manager by using the vProxy appliance. The instructions in this section assume that the vCenter server and the Platform Services Controller (PSC) are deployed as virtual machines.

For the restores to complete successfully:

- Ensure that these virtual machines use a fully qualified domain name (FQDN) with correct DNS resolution.
- Ensure that the host name of the machine is configured as an IP address. Note that if the host name is configured as an IP address, the IP address cannot be changed.

There are mainly two types of vCenter deployments:

- vCenter server Appliance/Windows Virtual Machine with an embedded PSC.
- vCenter server (also multiple) Appliance/Windows virtual machine with an external PSC.

This type has two sub categories:

- vCenter server environment with a single external PSC.
- vCenter server environment with multiple PSC instances. This environment contains multiple vCenter server instances registered with different external PSC instances that replicate their data.

Protecting an embedded PSC

The following section describes backup and recovery options for protecting an embedded PSC.

Backup

You can perform a backup of an embedded PSC by using the following guidelines.

1. Create a protection policy, and then add the vCenter virtual machine to the protection policy.
2. Select the full virtual machine and not individual disks.
3. Run the scheduled or on-demand (ad-hoc) protection policy.

Recovery

Depending on the type of failure, you can perform the virtual machine recovery by using one of the following methods.

- Restore to original — This method is valid only when the vCenter Server Appliance (VCSA) is intact and running, but corrupted.
- Recover as a new virtual machine to a managed ESXi server (Virtual Machine Recovery). Use this method if you have completely lost your VCSA. Note that this vCenter must be registered with PowerProtect Data Manager.
- Direct restore to ESXi server. Direct restore to ESXi will be the main use case.

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.

Prerequisites

Direct Restore to ESXi restore requires either the embedded VM Direct engine with PowerProtect Data Manager, or an external VM Direct appliance that is added and registered to PowerProtect Data Manager.


Additionally, ensure that you disconnect the ESXi host from the vCenter server.

Steps

1. From the PowerProtect Data Manager UI, select **Restore > Assets**, and then select the **Virtual Machine** tab.

The **Restore** window displays all of the virtual machines available for restore.

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 or click the **File Search** button to search on specific criteria.

The **Restore > 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 DD system, the copies on that system display in the right pane.

3. If the backup is on a DD 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. For low-bandwidth environments, select **Enable DDBoost Compression**.
This option reduces network usage by compressing data on the protection storage system before transfer to the VM Direct Engine, which decompresses the data. Compression reduces restore times but increases CPU usage on both systems.
 - c. Click **Next**.
6. On the **ESX Host Credentials** page:
 - a. In the **ESX Host** field, type the IP of the ESXi server where you want to restore the virtual machine backup.
 - b. Specify the root **Username** and **Password** for the ESXi 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.


Protecting external deployment models

Review the backup and recovery options for protecting external deployments.

Backup

You can perform a backup by using the following guidelines:


1. Create one protection policy and add the vCenter virtual machine and PSC virtual machine to the policy. This will ensure that snapshots are taken at the same time.
2. Ensure that you select the full virtual machine and not individual disks.
3. Run the scheduled or on-demand (ad-hoc) protection policy.

 **NOTE:** Ensure that you back up all vCenter server and PSC instances at the same time

Recovery

Depending on the failure, you can perform virtual machine recovery by using one of the following methods:

- Restore to original — This method is valid only when the VCSA is intact and running, but corrupted.
- Recover as a new virtual machine to a managed ESXi server: Use this method if you have completely lost your VCSA. Note that the vCenter where the VCSA resides must be registered with PowerProtect Data Manager.
- Emergency recovery to an ESXi server. For Emergency recovery, perform the steps specified in the section [Direct restore to ESXi](#) on page 122.

 **NOTE:** In the event of a complete environment failure, PSC should be restored first, followed by the vCenter server restore.

The following scenarios provide specific instructions based on the number of vCenter server appliances and external PSCs in the environment and the extent of the failure.

vCenter server appliance(s) with one external PSC where PSC fails

Steps

1. Perform an image-level recovery of the PSC by using one of the methods indicated above, and then power ON the virtual machine.
2. Verify that all PSC services are running.
 - For a PSC deployed as an appliance, run the **service-control --status --all** command in the appliance shell.
 - For a PSC installed on Windows, from the Windows Start menu, select **Control Panel > Administrative Tools > Services**.
3. Log into the vCenter server appliance shell as **root**.
4. Verify that no vCenter services are running, or stop any vCenter services that are running by typing **service-control --stop**.
5. Run the vc-restore script to restore the vCenter virtual machines.
 - For a vCenter server appliance, type **vc-restore -u psc_administrator_username -p psc_administrator_password**
 - For a vCenter Server installed on Windows, go to `C:\Program Files\VMware\vCenter Server\`, and then run **vc-restore -u psc_administrator_username -p psc_administrator_password**

where *psc_administrator_username* is the vCenter Single Sign-On administrator user name, which must be in UPN format.
6. Verify that all vCenter services are running and the vCenter Server is started, as specified in step two.
7. Perform a log in test to the vCenter Server.

If the restore was successful, the login completes successfully.


vCenter server appliance is lost but the PSC remains

Steps


1. Perform an image-level recovery of the lost vCenter server by using one of the following methods, and then power ON.
 - Restore to original — This method is valid only when the VCSA is intact and running, but corrupted.
 - Recover as a new virtual machine to a managed ESXi server — Use this method if you have completely lost your VCSA. Note that this vCenter must be registered with PowerProtect Data Manager.
 - Emergency recovery to an ESXi server.
2. After a successful boot, verify that all services are started.
3. Perform a log in test.

vCenter server appliance with multiple PSCs where one PSC is lost, one remains

Steps

1. Repoint the vCenter instance (insert link) to one of the functional PSC in the same SSO domain.
 **NOTE:** Log in to all vCenter servers one by one to determine which vCenter log in fails. This will be the vCenter that requires the repoint steps.
2. Run the following command on the vCenter server appliance:

```
cmsso-util repoint --repoint-psc psc_fqdn_or_static_ip [--dc-port port_number]
```



 **NOTE:** The square brackets enclose the command options.
3. Perform a log in test on the vCenter server.
4. Deploy the new PSC and join to an active node in the same SSO and site, replacing lost ones.
5. Repoint the vCenter server to the new PSC.

vCenter server appliance remains but all PSCs fail

About this task

 **NOTE:** In this scenario, none of the vCenter logins (SSO user) have been successful.

Steps

1. Restore the most recent PSC backup and wait for the vCenter services to start
2. Log in to the vCenter server appliance's shell as **root**.
3. Verify that no vCenter services are running, or stop vCenter services.
4. Run the **vc-restore** script to restore the VCSA (refer above for detailed steps).
 **NOTE:** If the login test to any vCenter server appliance fails, then the restored PSC is not the PSC that the vCenter server appliance is pointing to, in which case you may be required to perform a repoint, as described above.
5. Deploy the new PSC and join to an active node in the same SSO domain and site.
6. Repoint vCenter connections as required

vCenter server appliance remains but multiple PSCs fail


Steps

1. Restore one PSC.

2. Test the vCenter server appliance login. If the login fails, repoint the vCenter server appliance to an active PSC.
3. Deploy the new PSC and join to an active node in the same SSO domain and site.

vCenter server appliance fails

About this task

 **NOTE:** If a total failure has occurred (all PSCs and all vCenter server appliances failed), restore one PSC first before restoring the vCenter server appliance.

Steps

1. Perform an image-level restore of the lost vCenter server by using one of the following methods, and then power ON the vCenter.
 - Restore to original — This method is valid only when the vCenter server appliance is intact and running, but corrupted.
 - Recover as a new virtual machine to a managed ESXi server — Use this method if you have completely lost your vCenter server appliance. Note that this vCenter must be registered with PowerProtect Data Manager.
 - Emergency recovery to an ESXi server.
2. After a successful boot, verify that all vCenter services have started.
3. Perform a log in test.
4. If the log in test fails, then this vCenter server appliance is pointing to an inactive PSC. Repoint to an active node.

vCenter server restore workflow

The following diagram shows the restore workflow for a vCenter server.

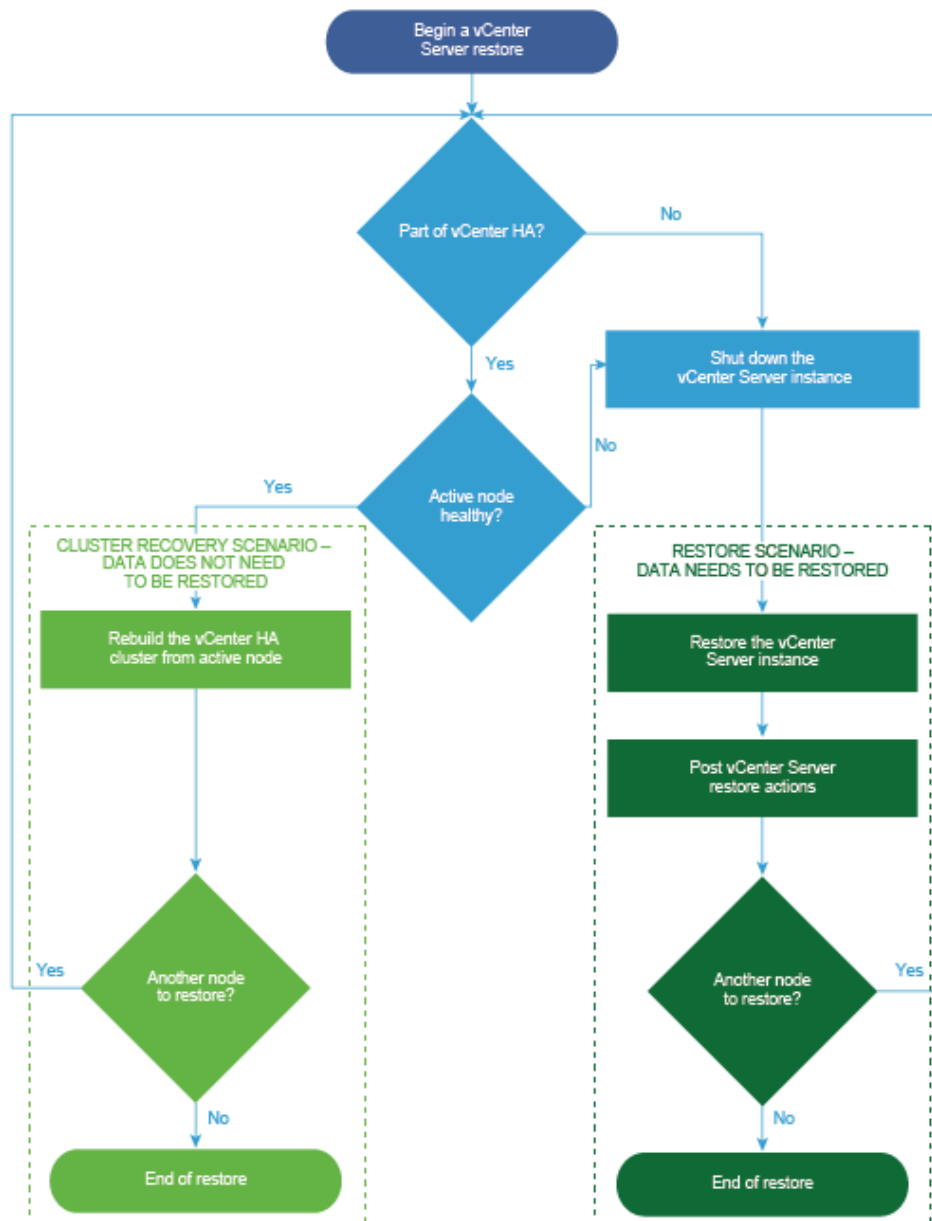


Figure 14. vCenter server restore workflow

Platform Services Controller restore workflow

The following diagram shows the restore workflow for a Platform Services Controller (PSC).

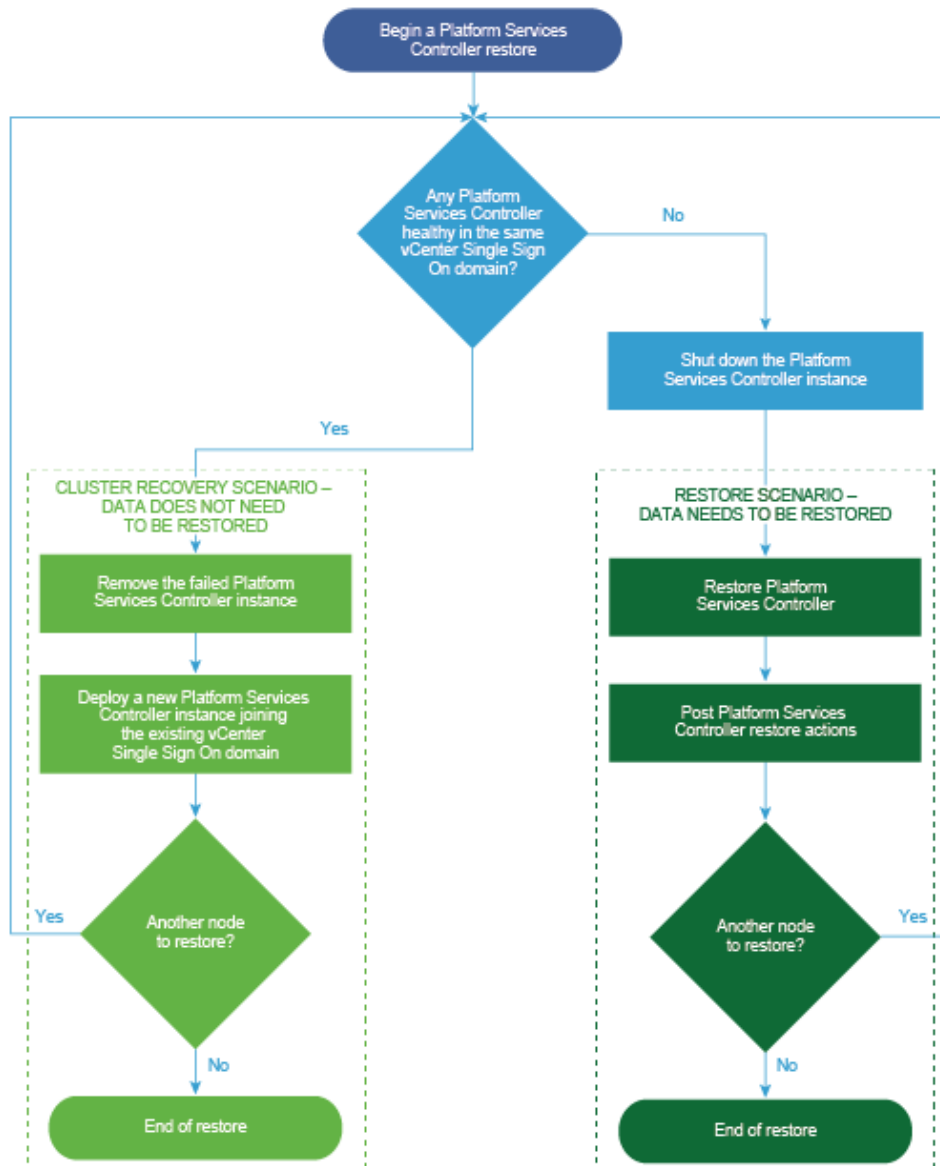


Figure 15. PSC restore workflow

Additional considerations

Review the following additional considerations when backing up and restoring the vCenter server and PSC.

- Backing up the vCenter server will not save the Distributed switch (vDS) configuration as it is stored on the hosts. As a best practice, back up the vDS configuration by using a script that can be used after restoring the virtual center.
- After restoring the PSC, verify that replication has been performed as designed by using the following commands to display the current replication status of a PSC and any of the replication partners of the PSC:
 - For VCSA, go to `/usr/lib/vmware-vmmdir/bin` and type `./vdcadmin -f showpartnerstatus -h localhost -u administrator -w Administrator_Password`
 - For Windows, open a command prompt and type `cd "%VMWARE_CIS_HOME%\vmmdir\`
- For the vCenter server or PSC, do not select advanced quiesce-based backup options. Selecting these options will result in application quiescing on virtual machines, which impacts the overall environment due to stuning.

The VMware vCenter server documentation, available at <https://docs.vmware.com/en/VMware-vSphere/index.html>, provides more information about the vCenter server and PSC.

Command reference

Use the following command to start or stop services in the vCenter server/PSC, or obtain the status:

```
service-control -status/start/stop -all
```

You can use other Replication topology commands, as in the following example.

Replication topology command

```
/usr/lib/vmware-vmdir/bin/vdcrepadmin -f showpartners -h localhost -u PSC_Administrator -w password
```

 **NOTE:** You can replace **localhost** with another PSC FQDN to obtain all of the partnerships in the current vSphere domain.


Backing Up VMware Cloud Foundation (VCF) on VxRail

Topics:

- [Backing up VCF on VxRail](#)
- [VCF and VxRail overview](#)
- [VCF components and backup methods](#)
- [Check VMware certification](#)
- [Backup prerequisites](#)
- [The backup script](#)
- [Quick protection](#)
- [Selective protection: SDDC and NSX-T Managers](#)
- [Selective protection: vCenter servers](#)
- [Selective protection: vRSLCM, VxRail Manager, Workspace ONE Access, and vRealize Suite virtual machines](#)
- [SFTP password change: SDDC and NSX-T Managers](#)
- [SFTP password change: vCenter servers](#)
- [Backup-script troubleshooting](#)

Backing up VCF on VxRail

The following sections describe how to protect VMware Cloud Foundation (VCF) on VxRail by using a PowerProtect Data Manager command-line backup script.

 **NOTE:** VxRail is the preferred Dell EMC platform for VCF. However, environments that use other VMware-supported vSAN Ready Nodes are also supported by Dell EMC. The following sections also apply to those environments.

VCF and VxRail overview

VCF integrates a VMware cloud infrastructure with cloud management services by using the vRealize software suite to run enterprise applications. The VCF infrastructure is managed by the SDDC Manager, and it includes vSphere compute, vSAN storage, NSX networking, and a range of security implementations.

Dell EMC VxRail is an all-in-one solution that uses Dell EMC PowerEdge servers and its own VxRail hyperconverged infrastructure (HCI) software to provide a fully functional VCF environment to enterprise customers.

For more information about VCF and VxRail, see the following resources:

- [The VMware Cloud Foundation documentation](#)
- [The Dell EMC VxRail Administration Guide at Customer Support](#)
- [About VMware Cloud Foundation on Dell EMC VxRail](#)

VCF components and backup methods

Understanding the backup method used by a VCF component aids in understanding how the VCF component is protected by the backup script. The following tables show the VCF components of the different backup methods.

Table 53. VCF components of file-based backups

Backup Method	Component
File based	NSX-T Data Center
	SDDC Manager
	vCenter Server

- Assets of these components are first copied to an external server that uses secure file transfer protocol (SFTP) or another supported protocol. After that, the external server is backed up by PowerProtect Data Manager.
- If using quick protection, these components are automatically protected.

Table 54. VCF components of image-based backups

Backup Method	Component	Automatically discovered
Image based	vRealize Suite LifeCycle Manager (vRSLCM)	VCF 4.0
	vRealize Automation	VCF 4.1
	vRealize Business	No
	vRealize Log Insight	VCF 4.1
	vRealize Network Insight	No
	vRealize Operations Manager	VCF 4.1
	VxRail Manager	No
	Workspace ONE Access	VCF 4.1

- Assets of these components are backed up directly by PowerProtect Data Manager.
- The **Automatically discovered** column displays the minimum required version of VCF for a component to be automatically discovered, as well as those components that are not automatically discovered by any version of VCF.
- If using quick protection, the automatically discovered components are automatically protected.

All image-based backups follow the [VMware quiescing recommendations](#) for VCF virtual machines that are part of VMware Validated Design (VVD):

Table 55. VCF components and quiescing


Component	Quiescing
vRealize Suite Lifecycle Manager	Enabled
Workspace ONE Access	Enabled
vRealize Log Insight	Disabled
vRealize Operations Manager	Disabled
vRealize Automation	Enabled

Check VMware certification

Use this method to check the versions of PowerProtect Data Manager that VMware has certified to work with their products.

About this task

VMware certification allows customers to receive support from VMware for any VMware-specific features related to PowerProtect Data Manager.

 **NOTE:** VMware will only certify a version of PowerProtect Data Manager after it has been released and tested. If you are waiting for the current version of PowerProtect Data Manager to be certified, you can continue to check its status.

Steps

1. In a browser, navigate to the [VMware Compatibility Guide](#).
2. Select **All > Dell EMC > All**.
3. Click **Update and View Results**.
4. In the **Solution Name** column, look for *EMC PowerProtect Data Manager* entries.
5. Review the information in the corresponding **Solution Version** and **Supported Releases** columns.

Backup prerequisites


Ensure the following prerequisites are met before backing up VCF on VxRail:

- VCF is at a supported version. For more information, see the PowerProtect Data Manager compatibility matrix at the [E-Lab Navigator](#).
- Any external server (using SFTP or another supported protocol) used in a file-based backup has been discovered as a File System asset in PowerProtect Data Manager.
- Any vCenter server being protected has been added as an asset source in PowerProtect Data Manager.
- PowerProtect Data Manager and the vCenter, SDDC, and NSX-T managers are all set to the same time zone and have their clocks synchronized.
- PowerProtect Data Manager and VCF do not have backup schedules that would back up the same assets at the same time.
- A VM Direct Engine exists.
- Any backup directory path specified by an external server in a file-based backup exists.
- All credentials provided during the execution of the backup script resolve to accounts with the required permissions to access the related resources.

The backup script

You use a PowerProtect Data Manager script to protect VCF components.

The script is accessible from the PowerProtect Data Manager command line. It provides a series of guided procedures that automate multiple backup operations into a single process. The script can also be used to change external SFTP passwords.

 **NOTE:** This script only backs up the data of protected VCF components. It cannot be used to restore any of the data that is backed up. To restore the data, use the PowerProtect Data Manager and VMware user-interface tools. Ensure that you restore VCF-management data to components in a manner supported by VMware. For more information, go to the [VMware Validated Design Documentation](#) website and review the backup and restore procedures of the documentation that corresponds to your version of VCF.

Quick protection

This procedure uses default backup settings and values to protect all VCF components at once. Every vCenter server and any automatically discovered VCF component will be protected. Quick protection requires the least amount of input, but also provides the least amount of choice. For information about the default settings and values used, review the selective-protection procedures that follow.

Steps

1. From a PowerProtect Data Manager command line, type the following two commands:

```
cd /usr/local/brs/lib/sysmgr/bin  
./ppdm-vcf-component-protection.sh
```

2. Enter credentials for the PowerProtect Data Manager server.
3. Enter the IP address or fully qualified domain name (FQDN) of the SDDC Manager server, and then enter credentials for the SDDC Manager server.
4. From the backup-script main menu, enter **1**.

i NOTE: Quick protection uses the same external SFTP server and backup schedule for both the SDDC Manager and vCenter servers. It also overrides the existing backup configurations of the SDDC and vCenter servers without prompting.

5. Enter the address of an external SFTP server, including the backup directory path, followed by credentials to access the server. The external SFTP server is also used for vCenter server configuration.

The external SFTP server and backup directory path uses the format **sftp://server_ip_address:port_number/folder/subfolder**. For example:

```
sftp://172.17.62.201:22/upload/backup
```

6. Enter the encryption passphrase for SDDC Manager backups.

The encryption passphrase must be between 12 and 32 characters in length and contain at least two lowercase letters, two uppercase letters, two numbers, and a special character.

i NOTE: The encryption passphrase is also used for vCenter server backups, and is required when restoring data. Store the passphrase in a secure location that is separate from the backup files and VCF environment you are protecting.

7. Confirm if common credentials should be used.
 - Enter **y** to provide common credentials for all vCenter servers.
 - Enter **n** to be prompted for the credentials for each individual server.
8. Select the days of the week a backup takes place, and then enter the time of day.

Type a number that represents a day of the week, where **1** represents Sunday. If selecting multiple days of the week, separate the numbers with a space. For example, to select Sunday and Monday:

```
1 2
```

The time of day uses the format **HH:MM** in 24-hour notation. For example, to enter 1:25 p.m.:

```
13:25
```

9. Select both a File System and Virtual Machine protection policy to use.
 - If a default protection policy of either type does not exist, it will be automatically created with a frequency of **DAILY**, a time of **8:00 PM** to **6:00 AM**, and a retention of **7** days.
 - A protection policy with the name *VCF-Image-Based-Protection* is used as the default image-based protection policy.
 - A protection policy with the name *VCF-File-Based-(SFTP)-Protection* is used as the default file-based protection policy.
 - If a default protection policy has just been automatically created and it is the only protection policy of that type, it will be automatically used.
 - If a default protection policy already exists, confirm if it should be used or if the protection policy to use should be selected from a list.
10. Enter the IP address or FQDN of any image-based VCF component that is not automatically discovered and that you want to protect. For a list of components that are not automatically discovered, see [VCF components and backup methods](#) on page 236.

Results

You can monitor the progress of the backup script as it protects the VCF components.

Selective protection: SDDC and NSX-T Managers

This procedure protects just the SDDC and NSX-T manager file-based VCF components, while providing more control over the backup settings used for them than quick protection. To protect other VCF components, refer to the other selective-protection procedures.

Steps

1. From a PowerProtect Data Manager command line, type the following two commands:

```
cd /usr/local/brs/lib/sysmgr/bin
./ppdm-vcf-component-protection.sh
```


2. Enter credentials for the PowerProtect Data Manager server.
3. Enter the IP address or fully qualified domain name (FQDN) of the SDDC Manager server, and then enter credentials for the SDDC Manager server.
4. From the backup-script main menu, enter **2**, and then **1**.
5. To override an existing SDDC Manager backup configuration, enter **y**.
6. To add or modify SDDC Manager backup configuration information, enter the address of an external SFTP server, including the backup directory path, followed by credentials to access the server.

The external SFTP server and backup directory path uses the format **sftp://server_ip_address:port_number/folder/subfolder**. For example:


```
sftp://172.17.62.201:22/upload/backup
```

7. Enter the encryption passphrase for SDDC Manager backups.

The encryption passphrase must be between 12 and 32 characters in length and contain at least two lowercase letters, two uppercase letters, two numbers, and a special character.

 **NOTE:** The encryption passphrase is required when restoring data. Store this passphrase in a secure location that is separate from the backup files and VCF environment you are protecting.

8. The default SSH fingerprint of the external SFTP server is displayed. Confirm that it should be used, or enter a new one.

 **NOTE:** With quick protection, the default SSH fingerprint of the external SFTP server is always used.

9. Select the backup frequency. If you select **HOURLY**, enter the minute of each hour a backup takes place. If you select **WEEKLY**, select the days of the week a backup takes place, and then enter the time of day.

For a weekly backup frequency, type a number that represents a day of the week, where **1** represents Sunday. If selecting multiple days of the week, separate the numbers with a space. For example, to select Sunday and Monday:

1 2

The time of day uses the format **HH:MM** in 24-hour notation. For example, to enter 1:25 p.m.:

13:25

10. Enter the backup-retention values described in the following table. The values automatically used by quick protection are also listed.

Table 56. Backup-retention values

Parameter	Value range	Quick-protection default value
Days of daily backups to retain	0–30	7
Days of hourly backups to retain	0–14	7
Backup files to retain	1–600	15
Take backups on state change	Yes or no	Yes

11. Confirm if a new File System protection policy should be created in order to protect the external SFTP server.

- Enter **y** to provide details of the new protection policy.
- Enter **n** to either select from a list of existing protection policies or skip protection of the external SFTP server.

Results

You can monitor the progress of the backup script as it protects the selected VCF components.

Selective protection: vCenter servers

This procedure protects just the vCenter server file-based VCF components, while providing more control over the backup settings used for them than quick protection. To protect other VCF components, refer to the other selective-protection procedures.

Steps

1. From a PowerProtect Data Manager command line, type the following two commands:

```
cd /usr/local/brs/lib/sysmgr/bin
./ppdm-vcf-component-protection.sh
```

2. Enter credentials for the PowerProtect Data Manager server.
3. Enter the IP address or fully qualified domain name (FQDN) of the SDDC Manager server, and then enter credentials for the SDDC Manager server.
4. From the backup-script main menu, enter **2** twice.
5. Select the automatically discovered vCenter servers to protect.

Enter **a** to protect all the servers. Otherwise, enter the numbers that correspond to the individual servers to protect, separating each number with a space.

6. Enter the address of an external server, including the backup directory path, followed by credentials to access the server.

Supported protocols for the external server are FTP, SFTP, FTPS, HTTP, HTTPS, NFS, and SMB. The external server and backup directory path uses the format **protocol://server_ip_address:port_number/folder/subfolder**. For example:

```
sftp://172.17.62.201:22/upload/backup
```

7. Select the days of the week a backup takes place, and then enter the time of day.


Type a number that represents a day of the week, where **1** represents Sunday. If selecting multiple days of the week, separate the numbers with a space. For example, to select Sunday and Monday:

```
1 2
```

The time of day uses the format **HH:MM** in 24-hour notation. For example, to enter 1:25 p.m.:

```
13:25
```


8. Confirm if the backups should be encrypted. If they should be encrypted, enter an encryption password.
If you enter an encryption password, it must be between 8 and 20 characters in length and contain at least one lowercase letter, one uppercase letter, one number, and one special character.
9. Confirm if historical data should be backed up and the number of backups to retain.

 **NOTE:** In quick protection, the default is to back up historical data and retain all backups.

10. Confirm if common credentials should be used.

- Enter **y** to provide common credentials for all vCenter servers.
- Enter **n** to be prompted for the credentials for each individual server.

11. If there is an existing vCenter server backup configuration, confirm if it should be overridden.

 **NOTE:** Should the existing backup configuration fail to be overridden, the vCenter server will be left without a backup configuration.

12. Confirm if a new File System protection policy should be created in order to protect the external server.

- Enter **y** to provide details of the new protection policy.
- Enter **n** to either select from a list of existing protection policies or skip protection of the external server.

Results

You can monitor the progress of the backup script as it protects the selected VCF components.

Selective protection: vRSLCM, VxRail Manager, Workspace ONE Access, and vRealize Suite virtual machines


This procedure protects all of the image-based VCF components, while providing more control over the backup settings used for them than quick protection. The components protected include vRSLCM, VxRail Manager, Workspace ONE Access, and vRealize Suite virtual machines. To protect file-based VCF components, refer to the other selective-protection procedures.

Steps

1. From a PowerProtect Data Manager command line, type the following two commands:

```
cd /usr/local/brs/lib/sysmgr/bin
./ppdm-vcf-component-protection.sh
```

2. Enter credentials for the PowerProtect Data Manager server.
3. Enter the IP address or fully qualified domain name (FQDN) of the SDDC Manager server, and then enter credentials for the SDDC Manager server.
4. From the backup-script main menu, enter **2**, and then **3**.
5. Select an image-based VCF component type to protect.

 **NOTE:** You can only select a single component type. To protect more than one component, follow the selective protection steps for each component.

- If you select vRSLCM, select a discovered vRSLCM server to protect.
 - If you select any other component type, enter the IP address or fully qualified domain name (FQDN) of the server to protect.
6. Confirm if a new Virtual Machine protection policy should be created in order to protect the component.
 - Enter **y** to provide details of the new protection policy.
 - Enter **n** to select from a list of existing protection policies.

Results

You can monitor the progress of the backup script as it protects the selected VCF component.

SFTP password change: SDDC and NSX-T Managers

While using the backup script to protect VCF components, you might want to change the password of the external SFTP server account associated with the SDDC and NSX-T Managers.

Steps

1. From a PowerProtect Data Manager command line, type the following two commands:

```
cd /usr/local/brs/lib/sysmgr/bin
./ppdm-vcf-component-protection.sh
```

2. Enter credentials for the PowerProtect Data Manager server.

3. Enter the IP address or fully qualified domain name (FQDN) of the SDDC Manager server, and then enter credentials for the SDDC Manager server.
4. From the backup-script main menu, enter **3**, and then **1**.
5. Confirm if you want to change the password of the external SFTP server account.
 - Enter **y** to change the password, and then perform the following actions:
 - a. Enter the new password.
 - b. Enter **y** to confirm if the automatically generated SSH fingerprint should be used. Otherwise, enter **n** to provide your own SSH fingerprint.
 - Enter **n** to skip the password change.

Results

You can monitor the progress of the backup script as it changes the password of the external SFTP server account associated with the SDDC and NSX-T managers.

SFTP password change: vCenter servers

While using the backup script to protect VCF components, you might want to change the password of an external SFTP server associated with an automatically discovered vCenter server.

Steps

1. From a PowerProtect Data Manager command line, type the following two commands:

```
cd /usr/local/brs/lib/sysmgr/bin
./ppdm-vcf-component-protection.sh
```
2. Enter credentials for the PowerProtect Data Manager server.
3. Enter the IP address or fully qualified domain name (FQDN) of the SDDC Manager server, and then enter credentials for the SDDC Manager server.
4. From the backup-script main menu, enter **3**, and then **2**.
5. Confirm if common credentials should be used.
 - Enter **y** to provide common credentials for all vCenter servers.
 - Enter **n** to be prompted for the credentials for each individual server.
6. Confirm if you want to provide a backup encryption password. This password will be used when backing up the VCF components of all vCenter servers.
7. For each automatically discovered vCenter server, confirm if you want to change the password of the external SFTP server account associated with it.

Results

You can monitor the progress of the backup script as it changes the passwords of all external SFTP server accounts associated with the selected vCenter servers.

Backup-script troubleshooting

The following table provides common error codes and messages, along with explanations or recommended areas of investigation to resolve the problem.

Table 57. Error codes and explanations

Error code or message	Explanation or area of investigation
INVALID_ENCRYPTION_PASSPHRASE Provided encryption passphrase <passphrase> is invalid.	The encryption passphrase specified for external SFTP server is invalid.
Validate Backup Location Details FAILED	The backup location specified for the external SFTP server in the SDDC Manager backup configuration does not exist.
INPUT_PARAM_ERROR Failed to establish SFTP connection to <SFTP server> with username <username> on port <port>.	The credentials specified for the external SFTP server in the SDDC Manager backup configuration are incorrect.
INVALID_ARGUMENT The entered backup password does not adhere to the password requirements.	The encryption passphrase specified in the vCenter server backup configuration is invalid.
INVALID_ARGUMENT Plugin error occurred. Access to the backup server is denied. Check your credentials.	The password specified for the external server in the vCenter server backup configuration is incorrect.
UNAUTHENTICATED Authentication required. com.vmware.vapi.endpoint.method.authentication.required	The credentials specified for the vCenter server are incorrect.
Perform validations for backup server fingerprint FAILED	The SSH fingerprint specified for the external SFTP server in the SDDC Manager backup configuration is invalid.
SCHEDULING_SDDC_MANAGER_BACKUPS_FAILED_REASON_UNKNOWN Unexpected error occurred. Provided backup schedule not applied.	Check for errors on the SDCC Manager.

Table 57. Error codes and explanations (continued)

Error code or message	Explanation or area of investigation
<p>LOCK_NOT_AVAILABLE</p> <p>Lock is not available - SDDC Manager DEPLOYMENT lock to perform Backup & Restore operation.</p>	There are too many pending SDDC Manager jobs. Try running the backup script at another time.
<p>503</p> <p>The data store service is not available. Try again later.</p> <p>remediation timestamp <timestamp> path /api/v2/assets</p>	PowerProtect Data Manager assets cannot currently be queried. Try running the backup script at another time.
<p>503</p> <p>The service is not available. Try again later.</p> <p>remediation timestamp <timestamp> path /api/v2/protection-policies</p>	Protection policies cannot currently be queried. Try running the backup script at another time.

Best Practices and Troubleshooting

Topics:

- Base 10 standard used for size calculations in the PowerProtect Data Manager UI
- Best practices and additional considerations for the VM Direct Engine
- Best practices for vCenter Server backup and restore
- Changing the vCenter server FQDN
- Monitoring storage capacity thresholds
- Replacing security certificates
- Restarting PowerProtect Data Manager
- Scalability limits for vCenter Server, VM Direct Engine and DD systems
- Troubleshooting network setup issues
- Troubleshooting PowerProtect agent service installations
- Troubleshooting PowerProtect agent service operations
- Troubleshooting PowerProtect Data Manager software updates
- Troubleshooting storage units
- Troubleshooting virtual machine backup issues
- Troubleshooting virtual machine restore issues
- Troubleshooting vSphere Plugin deployments

Base 10 standard used for size calculations in the PowerProtect Data Manager UI

For size calculations (for example, asset size, the available space on storage systems), the PowerProtect Data Manager UI uses the Base 10 standard, which specifies the size in MB, GB, and TB.

Other components, however, might use the Base 2 standard, which specifies the size in MiB, GiB, and TiB. When there is a discrepancy in reported size, use the UI to obtain the most correct information.

Best practices and additional considerations for the VM Direct Engine

Review the following information for recommendations and best practices when adding a VM Direct protection engine in PowerProtect Data Manager.

Change the limit of instant access sessions

For DDOS versions 6.2 and higher, PowerProtect Data Manager uses the limit that the DD storage appliance reports, and manages concurrent instant access sessions based on the reported limit.


You can change the limit by modifying a configuration file to override the default value. Note that sessions that exceed the maximum concurrent sessions that are supported are canceled and retried. To change the number of concurrent sessions manually to match the capability of the underlying storage appliance, perform the following steps.

1. Log in to the PowerProtect Data Manager UI as a user with the Administrator role.
2. If not already created, create an `application.yml` file in the `/usr/local/brs/lib/vmdm/config/` directory.
 NOTE: The structure of this file requires that you separate fields into individual categories and sub categories, as shown in the following step.

3. In the `application.yml` file, change the instant access session parameter value to override the default value. For example:

```
recovery:
  queue:
    ia_session_allowance: 32
```

4. Run `vmadm stop` and then `vmadm start` to restart the `vmadm` service.

 **NOTE:** Ensure that no other virtual machine operations are running, such as protection and recovery.

Configuring a backup to support vSAN datastores

Backup and recovery functionality is supported for vSAN virtual machines.

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.

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 protection storage.
- Ensure that the virtual machine firewall has port rules for the protection storage.
- For application-aware backups, ensure that Microsoft SQL Server instances are enabled for data protection using a SYSTEM account, as described in the section "Microsoft application agent for SQL Server application-aware protection" of the *PowerProtect Data Manager for Microsoft Application Agent SQL Server User Guide*.

Disable vCenter SSL certificate validation

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.

 **CAUTION:** 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 a file named `cbs_vmware_connection.properties` in the `/home/admin` directory on the PowerProtect Data Manager appliance, with the following contents:

```
cbs.vmware_connection.ignore_vcenter_certificate=true
```

2. If not already created, create an `application.yml` file in the `/usr/local/brs/lib/vmdm/config/` directory.

 **NOTE:** The structure of this file requires that you separate fields into individual categories and sub categories, as shown in the following step.

3. In the `application.yml` file, add the following contents:

```
vmware_connection:
  ignore_vcenter_cert: true
```

```
discovery:
  ignore_vcenter_cert: true
```

4. Run `cbs stop` to stop the cbs service, and then `cbs start` to restart the service.
5. Run `vmadm stop` to stop the vmadm service, and then `vmadm start` to restart the service.
6. 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.

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. However, if the user does not have sufficient administrator privileges, the mount fails and the **FLR Agent** is not installed. 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 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/vproxysra/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

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.

 **NOTE:** The most up-to-date software compatibility information for PowerProtect Data Manager is provided in the E-Lab Navigator, available at <https://elabnavigator.emc.com/eln/modernHomeDataProtection>.

FLR Agent installation on Linux virtual machines

The **FLR Agent** installation on Linux virtual machines requires that you use the root account, or that you are a user in the operating system's local sudoers list. If credentials for any other user are provided for the target virtual machine, the **FLR Agent** installation fails, even if this user has privileges similar to a root user.

To allow a non-root user or group to perform the **FLR Agent** installation:

1. Provide sudo access to the following files at a minimum:
 - rpm command (SLES, RHEL, CentOS) and dpkg command (Debian/Ubuntu)
 - /opt/emc/vproxyra/bin/postinstall.sh
 - /opt/emc/vproxyra/bin/preremove.sh

Note the following additional requirements:

- The sudo user or group must be configured for no password prompt.
 - The sudo user or group must be provided with the no requiretty option.
 - To browse files for a file level restore when you have user elevation enabled, you must have the appropriate authority in the guest virtual machine operating system. For example, you must be permitted to run `vflrbrowse` using sudo without prompting for a password.
 - To perform a file-level restore when you have user elevation enabled, you must have the appropriate authority. For example, you must be permitted to run `vflrcopy` using sudo without prompting for a password.
2. On the Linux system, create the file `/etc/sudoers.d/linuxuser`, where *linuxuser* is the Linux login user, and then add the following contents to this file.

On CentOS, Red Hat, SuSE, OpenSuSE, and Oracle Linux platforms:

```
username ALL=NOPASSWD: /usr/bin/sudo, /usr/bin/rpm, /opt/emc/
vproxyra/bin/postinstall.sh, /opt/emc/vproxyra/bin/preremove.sh, /opt/emc/vproxyra/bin/
vflrbrowse, /opt/emc/vproxyra/bin/vflrcopy

Defaults:username !requiretty
```

On Ubuntu platforms:

```
username ALL=NOPASSWD: /usr/bin/sudo, /usr/bin/dpkg, /opt/emc/
vproxyra/bin/postinstall.sh, /opt/emc/vproxyra/bin/preremove.sh, /opt/emc/vproxyra/bin/
vflrbrowse, /opt/emc/vproxyra/bin/vflrcopy

Defaults:username !requiretty
```

Once you complete the **FLR Agent** installation on the target virtual machine using the root user account or a sudouser with the minimum file access requirements, you can perform file level restore operations as a non-root user on supported Linux platforms. To determine which Linux platforms are supported, review the compatibility information at <https://elabnavigator.emc.com/elab/modernHomeDataProtection>.

FLR Agent installation on Windows virtual machines

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 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**.

Installation of the **FLR Agent** 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.

FLR-supported platform and OS versions for virtual machine restores

File-level restore is supported for the following platforms and operating system versions only.

Platforms/operating systems are qualified for file-level restore support using the default file system for these platforms:

 **NOTE:** The most up-to-date software compatibility information for PowerProtect Data Manager is provided in the E-Lab Navigator, available at <https://elabnavigator.emc.com/elab/modernHomeDataProtection>.


- RedHat Enterprise Linux versions 6.x, 7.x, and 8.x
- SuSE Linux Enterprise Server versions 11.x and 12.x
- Debian version 9.1
- Ubuntu version 17.10
- CentOS version 7.2 and later
- Oracle Enterprise Linux version 7.2 and later
- Windows 7, 8, 10, Server 2008, 2012, 2016 (all 64-bit platforms and R2, where applicable), 2019 for FAT, and NTFS.

Ensure that the latest supported version of VMware Tools or open-vm-tools is installed on the guest operating system.

Support for Debian or Ubuntu operating system

vProxy 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 ext4 file systems.

Steps

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:

- msixexec.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.

PowerProtect Data Manager resource requirements in a VMware environment

Review the following minimum system requirements for PowerProtect Data Manager in a VMware environment (ESXi server).

- CPU—10 CPU cores
- Memory—18 GB RAM for PowerProtect Data Manager
- Seven disks with the following capacities:
 - Disk 1—100 GB
 - Disk 2—500 GB
 - Disks 3 and 4—10 GB each
 - Disks 5 through 7—5 GB each
- 1 GB network interface card (NIC)

NOTE: If you plan to use Cloud DR, your system must also meet the following requirements:

- CPU—14 CPU cores
- Memory—22 GB

Software and hardware requirements

The following table lists the required components for PowerProtect Data Manager and the VM Direct protection engine.

Table 58. PowerProtect Data Manager and VM Direct engine requirements

Component	Requirements	Notes
PowerProtect Data Manager with the VM Direct engine	Version 19.9 or later.	
vCenter Server	vSphere and ESXi versions 6.5, 6.7, 7.0, 7.0 U1 and later.	<p>Refer to the VMware documentation ESXi 6.5 and later minimum requirements for physical host requirements for the ESXi hosts.</p> <p>VMware has announced the end of general support for vSphere version 6.0. The Knowledge Base article at https://kb.vmware.com/s/article/66977 provides more information.</p> <p>Version 6.5 and later is required to perform Microsoft SQL Server application-aware protection. Also, file-level restore in the vSphere Client requires a minimum vCenter version 6.7 U1.</p> <p>Any new virtual machine protection policies use Transparent Snapshot Data Mover (TSDM) as the default protection mechanism instead of VADP, provided that the vCenter/ESXi Server that hosts the virtual machines is a minimum version of 7.0 U3 and the policy options selected for the virtual machine crash-consistent protection policy are supported by TSDM.</p>

Table 58. PowerProtect Data Manager and VM Direct engine requirements (continued)

Component	Requirements	Notes
VMware Tools	Version 10 or later.	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 before backup. Version 10.1 and later is required to perform Microsoft SQL Server application-aware protection.
PowerProtect DD System models and software	<ul style="list-style-type: none"> All models of PowerProtect DD System in production are supported. DD Operating System (DDOS) version 6.2 or later and the PowerProtect DD Management Center (DDMC). 	Make note of the hosts writing backups to your DD systems.
Web browser	Google Chrome	The latest version of the Google Chrome browser is recommended to access the PowerProtect Data Manager UI.

Support for backup and restore of encrypted virtual machines

Backup and restore of encrypted virtual machines is supported in PowerProtect Data Manager, with the following limitations:

- Restoring encrypted virtual machines to a different vCenter Server is not supported. You must perform the restore to the original virtual machine or a new virtual machine in the same vCenter.
- Restoring an encrypted virtual machine backup to a new virtual machine in the original vCenter Server will restore the virtual machine disks (VMDKs) in clear text if the VMDKs are not encrypted. The article "Virtual Machine Encryption" at <https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-E6C5CE29-CD1D-4555-859C-A0492E7CB45D.html> provides more information about manually changing the virtual machine policy to enable encryption of VMDKs.
- In order to use **Hot Add** transport mode, all VM proxies with access to the encrypted virtual machines datastore must be encrypted as well. For example, if encrypted virtual machines reside in an ESXi cluster, all VM proxies deployed on the cluster must also be encrypted.
- In order to backup and restore encrypted virtualization-based security (VBS) and virtual Trusted Platform Module 2.0 (vTPM) virtual machines, vCenter 7.0 U1 or later is required.

Transport mode considerations

Review the following information for recommendations and best practices when selecting a transport mode to use for virtual machine data protection operations and Tanzu Kubernetes guest cluster protection in PowerProtect Data Manager.

Hot Add transport mode recommended for large workloads

For workloads where full backups of large sized virtual machines or backups of virtual machines with a high data change rate are being performed, **Hot Add** transport mode provides improved performance over other modes. With **Hot Add** transport mode, a VM Direct Engine must be deployed on the same ESXi host or cluster that hosts the production virtual machines. During data protection operations, a VM Direct Engine capable of performing Hot Add backups is recommended. The following selection criteria is used during data protection operations:

- If a VM Direct Engine is configured in Hot Add only mode, then this engine is used to perform **Hot Add** virtual machine backups. If one or more virtual machines are busy, then the backup is queued until the virtual machine is available.
- If a virtual machine is in a cluster where the VM Direct Engine is not configured in **Hot Add** mode, or the VM Direct Engine with **Hot Add** mode configured is disabled or in a failed state, then PowerProtect Data Manager selects a VM Direct Engine within the cluster that can perform data protection operations in **NBD** mode. Any VM Direct Engine with **Hot Add** mode configured that is not in the cluster is not used.
- Any VM Direct Engine that is configured in **NBD** only mode, or in **Hot Add** mode with fallback to **NBD**, is used to perform **NBD** virtual machine backups. If every VM Direct Engine that is configured in **NBD** mode is busy, then the backup is queued until one of these engines is available.

- If there is no VM Direct Engine that is configured in **NBD** mode, or the VM Direct Engine with **NBD** mode configured is disabled or in a failed state, then the PowerProtect Data Manager embedded VM Direct engine is used to perform the **NBD** backup.

Other transport mode recommendations

Review the following additional transport mode recommendations:

- Use **Hot Add** 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 Engine on an ESXi host that has a path to the storage that holds the target virtual disks 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.
 - In order for backup and recovery operations to use **Hot Add** mode on a VMware Virtual Volume (vVol) datastore, the VM Direct proxy should reside on the same vVol as the virtual machine.
 - If you have vFlash-enabled disks and are using **Hot Add** 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 Engine to a host with vFlash already configured. Otherwise, backup of any vFlash-enabled disks fails with the error VDDK Error: 13: You do not have access rights to this file and the error on the vCenter server The available virtual flash resource '0' MB ('0' bytes) is not sufficient for the requested operation.
 - For sites that contain many virtual machines that do not support **Hot Add** requirements, Network Block Device (**NBD**) transport mode is used. This mode can cause congestion on the ESXi host management network. Plan your backup network carefully for large scale **NBD** installs, for example, consider configuring one of the following options:
 - Setting up Management network redundancy.
 - Setting up backup network to ESXi for **NBD**.
 - Setting up storage heartbeats.
- See <https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmw-vsphere-high-availability-whitepaper.pdf> for more information.
- If performing **NBD** backups, ensure that your network has a bandwidth of 10 Gbps or higher.

Virtual disk types supported

When planning your protection policies, ensure that PowerProtect Data Manager supports the disk types that you use in the environment.

PowerProtect Data Manager does not support the following disk types:

- First Class Disks
- Independent (persistent and nonpersistent)
- RDM Independent - Virtual Compatibility Mode
- RDM Physical Compatibility Mode

Additionally, Dell EMC recommends to avoid deploying VMs with IDE virtual disks, which degrades backup performance. Use SCSI virtual disks instead whenever possible. Note that you cannot use **Hot Add** mode with IDE Virtual disks. Backup of IDE Virtual disks is performed using NBD mode.

Virtual machine data change rate

The data change rate is the percentage of a virtual machine's data that changes between backups.

Data change rates directly impact the number of VM Direct Engines required to successfully complete the backup of all required virtual machines within the backup window. A daily data change rate of 3-4% is typical in a vSphere environment. Higher data change rates will require either a longer window to complete the backup, additional VM Direct Engines, or both.

VM Direct Engine data ingestion rate

The VM Direct Engine data ingestion rate is another parameter that directly impacts the number of VM Direct Engines required to successfully complete the backup of all required virtual machines within the backup window.

By default, each VM Direct Engine processes approximately 500 GB to 1TB of data per hour, subject to the deduplication and read throughput on the primary stack. A number of additional factors, however, can impact the actual data ingestion rate, including the following:

- The protection storage system being used for data protection operations.
- The type of storage media used for VM Direct Engine storage.
- Your network and/or SAN infrastructure and connectivity speed.

If data ingestion rates at your site are typically lower or higher than 500 GB per hour, you can add or delete VM Direct Engines as needed. You can also shorten or lengthen the backup window. By default, each VM Direct Engine is configured to handle the optimal number of concurrent VMDK backup jobs. Configuring each VM Direct Engine to allow fewer concurrent backup jobs would typically require deploying additional VM DirectEngines, but can result in more evenly distributed backup jobs among each VM Direct Engine.

Full (Level-0) backups typically take longer and consume more VM Direct Engine resources. Therefore, large new virtual machine deployments can impact the ability to complete all required backups within the time specified for the backup window. In order to allow the system to perform these full backups without interruption, where possible ensure that you implement a phased approach for large new virtual machine deployments. If a phased deployment is not possible, and the full backups do not complete before timeout of the backup window, you can also enable automatic retry of failed backups. The section [Restart a job or task automatically](#) on page 148 provides instructions. It is recommended that an administrator user monitor such workloads to ensure that the system can handle these workloads when the demand on resources begins to decrease, and that the virtual machine backups then complete successfully.

VM Direct Engine limitations and unsupported features

Review the following limitations and unsupported features related to the VM Direct Engine.

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.

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.

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.

DD Boost over fibre channel not supported

PowerProtect Data Manager does not support DD Boost over fibre channel (DFC).

Error when changing configuration of many virtual machines at the same time

When configuring or unconfiguring many 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 protection rules to automatically determine which assets are assigned to protection policies when the assets are discovered.

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)".
```

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.

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" of the *PowerProtect Data Manager for Microsoft Application Agent SQL Server User Guide*.

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.

NFC log level settings

To assist with I/O performance analysis, set the NFC log level in the VM Direct proxy configuration file to its highest value, for example, **vixDiskLib.nfc.LogLevel=4**. Setting the log level in the server for NFC asynchronous I/O is not required. You can then run the VDDK sample code and evaluate I/O performance by examining the `vddk.log` and the `vpxa` log file.

NOTE: Virtual Machines with very high I/O might stall 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.

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 or later installed, avoid using these two characters in virtual machine names.

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 Engine 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.

Thin provisioning not preserved during NFS datastore recovery

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 <https://kb.vmware.com/kb/2137818> provides more information.

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 <https://docs.vmware.com/en/VMware-vSphere/6.0/rn/vsphere-vcenter-server-60u2-release-notes.html> provide more information.

VM Direct Engine configuration settings cannot be modified after adding the VM Direct Engine

After adding a VM Direct Engine, 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 Engine. [Additional VM Direct actions](#) on page 68 provides more information.

VM Direct Engine configured with dual stack is not supported

The VM Direct Engine does not support dual stack (IPv4 and IPv6) addressing. If you want to run backups and restores using the VM Direct Engine, use IPv4 only addressing.

VMware Distributed Resource Scheduler cluster support limitations

The PowerProtect Data Manager server is supported in a VMware Distributed Resource Scheduler (DRS) cluster, with the following considerations:

- During backup of a virtual machine, `host-vmotion` or `storage-vmotion` is not permitted on the virtual machine. The option to migrate will be disabled in the **vSphere Client** UI.
- If the VM Direct proxy is in use for a backup or restore with **Hot Add** disks attached, then `storage-vmotion` of the vProxy is not permitted during these operations.

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>.

VMware snapshot for backup is not supported for independent disks

When using independent disks you cannot perform VMware snapshot for backup.

VM Direct Engine performance and scalability

The VM Direct Engine 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 59. Performance and scalability factors

Component	Maximum limit	Recommended count	Notes
Number of concurrent NBD + Preferred Hot Add backups per ESXi host	48		Ensure that your network has a bandwidth of 10 Gbps or higher. 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		180	Can be achieved with a combination of the number of proxies multiplied by the number of configured Hot Add sessions per VM Direct Engine.
Number of proxies per vCenter Server	25	7	A limit of 25 concurrent backup and recovery sessions.
Number of files/directories per file level recovery	200,000		File-level restore 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.

When you reach the limit for concurrent backup sessions, a warning message displays. The remaining sessions will be queued. You can adjust the session limits by modifying the `MAX_VC_BACKUP_SESSIONS` and `MAX_NBD_BACKUP_SESSIONS` variables in the environment file, according to the recommendations. The Knowledge Base article 543253 at <https://support.emc.com/kb/543253> provides more information.

Table 60. Proxy session limits by proxy type

Component	Total number of sessions (backup and recovery) maximum	Notes
Added (External) VM Direct Engine	25	
Embedded VM Direct engine  NOTE: The embedded VM Direct engine is pre-bundled with the PowerProtect Data Manager software.	4	The embedded VM Direct engine is only used as a fallback when all other proxies are disabled or in Failed state.

VM Direct Engine selection with virtual networks (VLANs)

PowerProtect Data Manager typically selects a VM Direct Engine by accounting for availability, transport mode settings, and engine load. This selection optimizes data throughput.

When you configure virtual networks for PowerProtect Data Manager and VM Direct Engine to isolate backup traffic, you can define routes to the protection storage system interface for each virtual network. The routes that you configure can influence VM Direct Engine selection. PowerProtect Data Manager ensures that the selected engine has a network interface that can send traffic for a specific virtual network to the protection storage system.

Best practices for vCenter Server backup and restore

Review the following recommendations and best practices when planning a vCenter Server backup and restore.

 **NOTE:** Backups will not save Distributed switch configurations.

- It is recommended to schedule the backup of the vCenter Server when the load on the vCenter Server is low, such as during off-hours, to minimize the impact of vCenter virtual machine snapshot creation and snapshot commit processing overhead.
- Ensure that there are no underlying storage problems that might result in long stun times.
- Keep the vCenter virtual machine and all of its component virtual machines in one single isolated protection policy. The protection policy should not be shared with any other virtual machines. This is to ensure that the backup times of all vCenter Server component virtual machines are as close to each other as possible.
- Ensure that the backup start time of the vCenter Server does not overlap with any operations for other protected virtual machines being managed by this vCenter so that there is no impact on other protected virtual machines during snapshot creation and snapshot commit of the vCenter virtual machine.
- If the vCenter Server and Platform Services Controller instances fail at the same time, you must first restore the Platform Services Controller and then the vCenter Server instances.

Changing the vCenter server FQDN

If you change the fully qualified domain name (FQDN) of the vCenter server, PowerProtect Data Manager must be reconfigured to accommodate this change without any issues.


When the FQDN of the vCenter server changes, so does its SSL certificate. In order to continue to administer the vCenter server and maintain uninterrupted protection of its assets, the new certificate must be imported into the PowerProtect Data Manager trust store.

Change the vCenter server FQDN

When the FQDN of the vCenter server changes, its new SSL certificate must be imported into the PowerProtect Data Manager trust store.

About this task

This procedure uses REST API commands that are run on the PowerProtect Data Manager server.

 **NOTE:** In the following steps, replace **192.168.1.204** with the IP address of the PowerProtect Data Manager server and **a022-renamed-ppdm.vmware.com** with the new FQDN of the vCenter server.

Steps

1. Get the current information from the vCenter server, and make a note of the value of *id*, which corresponds to the new FQDN certificate:

```
GET https://192.168.1.204:8443/api/v2/certificates?host=a022-renamed-ppdm.vmware.com&port=443&type=Host
```

For example, the output might look like this:

```
fingerprint: "43FF8FBA82D1DD68E630AE9DB8BA7DF21549CE39"
host: " a022-renamed-ppdm.vmware.com"
```

```
id: "dmNlbnRlci12bWRtLTA0LmFzbC5sYWluZWljLmNvbTo0NDM6aG9zdA=="
issuerName: "OU=VMware Engineering, O= a022-renamed-ppdm.vmware.com, ST=California, C=US, DC=local, DC=vsphere, CN=CA"
notValidAfter: "Mon Mar 11 17:39:09 PDT 2030"
notValidBefore: "Mon Mar 16 17:39:09 PDT 2020"
port: "443"
state: "UNKNOWN"
subjectName: "C=US, CN=vcenter-vmdm-04.asl.lab.emc.com"
type: "HOST"
```

2. Import the new certificate into the PowerProtect Data Manager trust store:

```
PUT https://192.168.1.204:8443/api/v2/certificates/{newCertID}
```

Replace *{newCertID}* with the value of *id* displayed in step 1. Only use the text that was displayed between the quotation marks.

3. Get the ID of the vCenter server:

```
GET https://192.168.1.204:8443/api/v2/inventory-sources/
```

All vCenter servers that are configured in PowerProtect Data Manager are displayed.

For example, the output might look like this:

```
"id": "6ffdb6e9-b864-56f4-8ec8-fe1c214c6fef",
  "name": "VC",
  "version": "7.0.2",
  "type": "VCENTER",
  "lastDiscovered": "2021-08-10T07:03:41.624Z",
  "lastDiscoveryResult": {
    "status": "OK",
```

4. Record the new FQDN of the vCenter server in PowerProtect Data Manager:

```
PUT https://192.168.1.204:8443/api/v2/inventory-sources/{vCenter-id}
```

Replace *{vCenter-id}* with the value of *id* displayed for the vCenter in step 3. Only use the text that was displayed between the quotation marks.

5. Get the current list of certificates:

```
GET https://192.168.1.204:8443/api/v2/certificates
```

Both the old and new FQDN certificates are displayed. There might also be additional certificates displayed.

6. Search the certificate entries displayed in step 5, and locate the entry where the value of *host* matches the old FQDN of the vCenter server. Make a note of the corresponding *id* value.

7. Delete the old certificate from the PowerProtect Data Manager :

```
DELETE https://192.168.1.204:8443/api/v2/certificates/{oldCertID}
```

Replace *{oldCertID}* with the value of *id* noted in step 6. Only use the text that was displayed between the quotation marks.

Monitoring storage capacity thresholds

PowerProtect Data Manager periodically monitors protection storage usage and reports alerts when a system reaches two capacity thresholds. As a best practice, check for these alerts and respond before the system exhausts storage capacity.

At 80% capacity, PowerProtect Data Manager generates a weekly warning alert. At this threshold, you should develop a strategy to add capacity or move protection policies to another storage target. [Managing Protection Policies](#) on page 73 provides more information about moving policies.

At 95% capacity, PowerProtect Data Manager generates a daily critical alert. At this threshold, capacity exhaustion is imminent. Changing the capacity alerting thresholds requires contacting Support.

Replacing security certificates

You can replace the default self-signed security certificates for the PowerProtect Data Manager UI, or replace changed or expired security certificates on an external server.

The *PowerProtect Data Manager Security Configuration Guide* provides more information.

Replacing the self-signed security certificates

If you want to use certificates for the PowerProtect Data Manager UI that are signed by a certificate authority (CA) of your choice, you can replace them.

The *PowerProtect Data Manager Security Configuration Guide* provides more information.

Replace expired or changed certificates on an external server

Use this procedure to replace certificates on an external server (for example, a DD, LDAPS, or vCenter server) that have expired or changed. Only the Administrator role can replace certificates.

About this task

If a certificate on the external server has expired or been changed, connection to the server fails with the following error:

```
javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX
```

Perform the following steps using cURL or any REST API client, such as Postman.

Steps

1. Log in to the external server as an administrator:

POST `https://server_hostname:REST_port_number/api/v2/login`

Provide the following request payload in JSON format:

```
{
  "username": "username",
  "password": "password"
}
```

where *username* is a user with the Administrator role and *password* is the password for this user.

NOTE: Add the following header key with your REST call request:

'Content-type: application/json'

The response returns the following information:

```
{
  "access_token":
  "token_type":
  "expires_in":
  "jti":
  "scope":
  "refresh_token":
}
```

Copy the **access_token** value from the response above. This value will be required in the header key **Authorization** for all the REST calls in subsequent steps.

2. On the REST API client, run the following to obtain the old or expired external server certificate:

GET `https://server_hostname:REST_port_number/api/v2/certificates`

NOTE: Add the following header key with your REST call request:

'Authorization: access_token_value'

The response returns a list of certificate entries, each containing the following information:

```
[{
  "id":
  "host":
  "port":
  "notValidBefore":
  "notValidAfter":
  "fingerprint":
  "subjectName":
  "issuerName":
  "state":
  "type":
}]
```

NOTE: Make note of the **host**, **port** and **type** of each certificate, as this information will be required in Step 4. If you supply incorrect information in Step 4, requests that use these external hosts might fail.

3. On the REST API client, delete the old or expired external server certificate from the PowerProtect Data Manager datastore, using the ID obtained from the response in step 2:

DELETE `https://server hostname:REST port number/api/v2/certificates/id`

NOTE: Add the following header key with your REST call request:

`'Authorization: access_token_value'`

Ensure that you delete only the external server certificate that you want to remove.

4. On the REST API client, obtain the new certificate from the external server, using the host, port, and type obtained from the response in step 2:

GET `https://server hostname:REST port number/api/v2/certificates?`
`host=host&port=port&type=type`

NOTE: Add the following header key with your REST call request:

`'Authorization: access_token_value'`

The response returns the following information:

```
[{
  "id":
  "host":
  "port":
  "notValidBefore":
  "notValidAfter":
  "fingerprint":
  "subjectName":
  "issuerName":
  "state": "UNKNOWN",
  "type":
}]
```

5. On the REST API client, accept the new certificate, using the ID obtained in the response from step 4:

PUT `https://server hostname:REST port number/api/v2/certificates/id`

NOTE: Add the following header key with your REST call request:

`'Authorization: access_token_value'`

Also, copy the response payload from step 4 in JSON format and change the state from **"UNKNOWN"** to **"ACCEPTED"**.

6. On the REST API client, verify that the new certificate has been accepted, using the ID obtained in the response from step 4:

GET `https://server hostname:REST port number/api/v2/certificates/id`

NOTE: Add the following header key with your REST call request:

`'Authorization: access_token_value'`

If the certificate was accepted, the response returns the following information:

```
[{
  "id":
  "host":
  "port":
  "notValidBefore":
  "notValidAfter":
  "fingerprint":
  "subjectName":
  "issuerName":
  "state": "ACCEPTED",
  "type":
}]
```

Restarting PowerProtect Data Manager

When a PowerProtect Data Manager restart is required, Dell Technologies recommends that you avoid directly powering off the virtual machine unless it is necessary.

To ensure that PowerProtect Data Manager is able to properly restart, use the `reboot` or `shutdown` command. For example, on Linux, run the command `shutdown -r` or `shutdown -h now`.

Scalability limits for vCenter Server, VM Direct Engine and DD systems

The following limits have been tested successfully with PowerProtect Data Manager for the vCenter Server, VM Direct Engine, and DD systems.




 **NOTE:** These numbers are not maximum or hard limits, but should be considered when scaling your environment.

Table 61. Scalability limits

Component	Tested limits
Number of vCenter Servers supported with a single PowerProtect Data Manager server	12  NOTE: The vCenter server limit is subject to the VM Direct Engine overall limit of 40 and the per vCenter server limit of 25. For example, using the maximum tested number of vCenter servers of 12, you could add an average of 3 VM Direct Engines per vCenter server.
Number of external VM Direct Engines supported with a single PowerProtect Data Manager server	40  NOTE: This number was tested across 10 vCenter servers. For example, 4 VM Direct Engines per vCenter server.
Number of DD systems supported per PowerProtect Data Manager server	10
Network latency between the PowerProtect Data Manager server and VM Direct Engines	200 ms
Network latency between the PowerProtect Data Manager server and the DD systems	200 ms
Number of virtual machines per PowerProtect Data Manager server	10,000

Troubleshooting network setup issues

vCenter registration and proxy deployment fails if the PowerProtect Data Manager server is deployed in the same private network as the internal Docker network.

PowerProtect Data Manager uses an internal private Docker network. If the PowerProtect Data Manager server is deployed in the same private network as the internal Docker network, or if some data sources have already been deployed within the private network, PowerProtect Data Manager fails to protect the data sources.

To resolve this issue, deploy the PowerProtect Data Manager server and other data sources in a different network. If you cannot modify the deployed network, run a script tool within PowerProtect Data Manager to switch the private Docker network to a different network.

To switch the private Docker network to a different network:

1. Connect to the PowerProtect Data Manager console and change to the root user.
2. Modify the Docker network by running the following command:

```
/usr/local/brs/puppet/scripts/docker_network_switch.sh subnet gateway
```

Where:

- *subnet* describes the new network in the format **172.25.0.0/24**
- *gateway* is the gateway for the private network. For example: **172.25.0.1**

Ensure that you specify a subnet and gateway that is not in use.

Troubleshooting PowerProtect agent service installations

A PowerProtect agent service installation might fail with the following error message:

```
Service 'PowerProtect Agent Service' (AgentService) could not be installed. Verify that you have sufficient privileges to install system services.
```

Possible causes of the installation failure are as follows:

- The installation was attempted on a passive node of a Failover Cluster Instance (FCI).
- The installation was canceled and a rollback left some stale entries of PowerProtect agent services.

As a workaround, clean up the PowerProtect agent service entries, and retry the installation.

Troubleshooting PowerProtect agent service operations

When investigating issues with the PowerProtect agent service, you might need to troubleshoot its operations.

Troubleshoot the PowerProtect agent service operations

To troubleshoot the agent service operations, you can check the agent service log file `OpAgentSvc-<timestamp>.log`, which is created in `<agent_service_installation_location>\logs` on Windows and `<agent_service_installation_location>/logs` on AIX or Linux. To modify the log level and retention of temporary files, you can modify specific parameter settings in the `config.yml` file.

About this task

To modify the log level and retention of temporary files, you can perform the following steps.

Steps

1. Stop the agent service by using the appropriate procedure from the preceding topic.
2. Open the `config.yml` file in an editor.
3. Modify the log-level settings in the following parameters, as required:

i **NOTE:** These parameters are listed in order of decreasing number of messages in the debug information output. The default log-level is `INFO`.

- `DEBUG`
- `INFO`
- `WARNING`
- `ERROR`
- `CRITICAL`

4. To retain the temporary files, set the `keepTempFiles` parameter to `True` in the `config.yml` file.

i **NOTE:** The agent service and application agent communicate through the temporary files, which are typically deleted after use but can be useful for troubleshooting purposes. Do not leave the `keepTempFiles` parameter set to `True` permanently, or the temporary files can use excessive space on the file system.

5. Start the agent service by using the appropriate procedure from the preceding topic.

Troubleshooting PowerProtect Data Manager software updates

Review the following information related to updating the PowerProtect Data Manager software.

Mounting a read-only file system results in a failed update

If you mount a read-only file system under the `/home/admin` or `/home/sysadmin` directories on the PowerProtect Data Manager node, the update cannot complete successfully. Ensure that you remove read-only file system mounts before updating PowerProtect Data Manager.

Managing certificates after updating PowerProtect Data Manager from versions earlier than 19.1

Use this procedure to ensure that certificates existing on the pre-update system also exist on the post-update system.

Prerequisites

Ensure that you update any expired certificates on external systems to valid certificates.

Steps

1. Connect to the PowerProtect Data Manager console as an admin user.
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.

Troubleshooting storage units

When you add a protection policy or create a storage unit in PowerProtect Data Manager, storage unit creation fails if you reach the maximum MTree and Users count on the selected DD system.

PowerProtect Data Manager enables you to finish adding a protection policy without a storage unit. However, if you subsequently run a backup with this protection policy, the backup process is suspended indefinitely with no error message.

To continue backup operations, you must perform a cleanup on the DD system.

Troubleshooting virtual machine backup issues

This section provides information about issues related to virtual machine backup operations with the VM Direct protection engine.

Backup completes with a non-quieted snapshot warning

A virtual-machine backup completes, but with a warning that a non-quieted snapshot was used. Although most data will be protected, using a non-quieted snapshot can result in some data being out of date or missing altogether.

The following warning is seen after a backup completes:

Warnings occurred during snapshot creation. Non-quieted snapshot was used, quieted snapshot was unsuccessful. Unable to create quieted snapshot: An error occurred while quieting the virtual machine. See the virtual machine's event log for details.


This can happen with backups of both Windows and Linux virtual machines. Refer to the following procedures for common methods of resolving the issue.

Troubleshooting non-quieted Windows snapshots

There is a common method of resolving this issue on Windows.

Steps

1. Confirm that the virtual machine has VMware Tools 10.1.0 or higher installed. If the virtual machine does not have VMware Tools 10.1.0 or higher installed, then install it.
2. Confirm that the *VMware Snapshot Provider* service is installed on the virtual machine. If the *VMware Snapshot Provider* service is not installed, then install it by reinstalling VMware Tools.

 **NOTE:** Antivirus software might interfere with the installation of this service. If it is still not installed after reinstalling VMware Tools, then temporarily disable any antivirus software and reinstall VMware Tools again.

Troubleshooting non-quieted Linux snapshots

There is a common method of resolving this issue on Linux.

Steps

1. At a shell prompt of the virtual machine, run the command `cat /etc/vmware-tools/tools.conf`, and look for the value of `enableSyncDriver`:

```
[root]# cat /etc/vmware-tools/tools.conf
[vmbackup]
enableSyncDriver = false
```

2. If the value of `enableSyncDriver` is `false`, perform the following steps:
 - a. Edit `/etc/vmware-tools/tools.conf`, and change `enableSyncDriver = false` to **`enableSyncDriver = true`**.
 - b. At the shell prompt, run the command `systemctl restart vmtoolsd.service`.

Backup fails when names include special characters

When spaces or special characters are included in the virtual machine name, datastore, folder, or datacenter names, the `.vmtx` file is not included in the backup.

The VM Direct appliance does not back up objects that include the following special characters (format: character/escape sequence):

- `&` %26
- `+` %2B
- `/` %2F
- `=` %3D
- `?` %3F
- `%` %25
- `\` %5C
- `~` %7E
- `]` %5D

Deleting vCenter asset sources or moving ESXi to another vCenter

When you delete a vCenter Server asset source from PowerProtect Data Manager without removing any vProxy/Search Nodes that the vCenter is hosting, the Nodes will become non-operational and move into Failed status upon the next health check. As a result, PowerProtect Data Manager updates will fail. This issue also occurs when you move the ESXi hosting the vProxy/Search Nodes from one vCenter to another vCenter.

To correct this issue, you can perform one of the following actions:

- Manually delete the vProxy/Search Nodes. The section [Delete vProxy/Search Nodes when vCenter Server asset source is no longer required](#) on page 266 provides the required steps.
- Return the vProxy/Search Nodes to an Operational/Ready state using the `vproxymgmt` and `infranodemgmt` tools. Choose this action if you want to add the vCenter again, or you want to add the vCenter that the ESXi has been moved to. The section [Return vProxy/Search Nodes to operational state when re-adding vCenter](#) on page 267 provides the required steps.

Delete vProxy/Search Nodes when vCenter Server asset source is no longer required

Perform the following procedure when you delete a vCenter server as an asset source in PowerProtect Data Manager and you will not be re-adding the vCenter:

About this task

 **NOTE:** Manual cleanup of the virtual machine for the vProxy/Search Node has to be performed from the vCenter Server.

Steps

1. Run the following command to source the environment file.
`source /opt/emc/vmdirect/unit/vmdirect.env`
2. For vProxy removal:
 - a. Obtain the list of vProxies that require removal by running `/opt/emc/vmdirect/bin/vproxymgmt get`
 - b. Make note of the ID of any vProxy that needs to be deleted.
 - c. Use the `vproxymgmt` tool to delete vProxies by running `/opt/emc/vmdirect/bin/vproxymgmt delete -vproxy_id ProxyID`
3. For Search Node removal:
 - a. Obtain the list of Search Nodes that require removal by running `/opt/emc/vmdirect/bin/infranodemgmt get`
 - b. Make note of the ID of any Search Node that needs to be deleted.
 - c. Use the `infranodemgmt` tool to delete Search Nodes by running `/opt/emc/vmdirect/bin/infranodemgmt delete -node_id NodeID`
4. In the PowerProtect Data Manager UI, ensure that any sessions have been removed for both the vProxy/Search Node.

Return vProxy/Search Nodes to operational state when re-adding vCenter

When you want to re-add a vCenter that you deleted from PowerProtect Data Manager, or you want to add a vCenter that an ESXi has been moved to, perform the following procedure in order to return the vProxy/Search Nodes to an Operational/Ready state.

Steps

1. Re-add the deleted vCenter as an asset source in the PowerProtect Data Manager UI, or note the name of the new vCenter where the ESXi has been moved.
2. Run the following command to source the environment file.

```
source /opt/emc/vmdirect/unit/vmdirect.env
```
3. For vProxy updates:
 - a. Obtain the list of vProxies that require updating by running `/opt/emc/vmdirect/bin/vproxymgmt get`
 - b. Make note of the ID of any vProxy that needs to be updated.
 - c. Use the `vproxymgmt` tool to update the vCenter name by running `/opt/emc/vmdirect/bin/vproxymgmt modify -vcenter_hostname vCenter-FQDN -vproxy_id ProxyID`
4. For Search Node updates:
 - a. Obtain the list of Search Nodes that require updating by running `/opt/emc/vmdirect/bin/infranodemgmt get`
 - b. Make note of the ID of any Search Node that needs to be updated.
 - c. Use the `infranodemgmt` tool to update the vCenter name by running `/opt/emc/vmdirect/bin/infranodemgmt modify -vcenter_hostname vCenter-FQDN -node_id NodeID`
5. In the PowerProtect Data Manager UI, ensure that any sessions for the vProxy/Search Node and Cluster have changed to Operational/Ready state.

Failed to lock Virtual Machine for backup: Another EMC vProxy operation 'Backup' is active on VM

This error message appears when a backup fails for a virtual machine or when a previous backup 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.

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 vProxy Session**.

Managing command execution for VM Proxy Agent operations on Linux

The VM Proxy 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 Proxy 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 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.

PowerProtect plug-in and portlet for vSphere display errors after replacing security certificates

After you replace the default self-signed security certificates, you may see errors in the vSphere client PowerProtect portlet when you select virtual machines:

- Service Unavailable: Please contact your administrator.
- No healthy upstream.

Reinstall the PowerProtect plug-in to apply the new certificates. The *PowerProtect Data Manager Security Configuration Guide* provides more information.

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 reasons outlined in the following table.

Table 62. 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.
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 support matrix available at <http://compatibilityguide.emc.com:8080/CompGuideApp/>.

SQL Server application-aware backup displays an error about `disk.EnableUUID` variable

Issue

A SQL Server application-aware virtual machine backup succeeds but displays the following error when the `disk.EnableUUID` variable for the virtual machine is set to `TRUE`:

```
VM '<asset_name>' configuration parameter 'disk.EnableUUID' cannot be evaluated. Map item 'disk.EnableUUID' not found. (1071)
```

Workaround

After you set the `disk.EnableUUID` variable to `TRUE`, reboot the virtual machine.

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**.

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.

VMware knowledge base articles and product documentation

Additional VMware troubleshooting information is available at the [VMware Knowledge Base](#) and [VMware Documentation](#) websites.

Troubleshooting virtual machine restore issues

The following topics provide information on troubleshooting virtual machine restore failures.

Virtual machine restores fail when vProxyd or vrecoverd disruption occurs

A virtual machine restore hangs and VPOD will not be able to reconnect to the restore session when the following scenarios occur:

- A disruption to the `vrecoverd` process on any external VM Direct engine.
- A disruption to the `vProxyd` process during a **Restore to Original Folder and Overwrite Original Files** or **Create and Restore to New VM** operation that uses Transparent Snapshot Data Mover (TSDM) as the protection mechanism.

After several retry attempts, VPOD marks the restore session as "Failed" and releases the vProxy associated with the restore.

If this failure occurs during a **Create and Restore to New VM**, you can delete the new virtual machine and restart the restore operation.

If this failure occurs during a **Restore to Original Folder and Overwrite Original Files**, you must remove the vProxy lock on the virtual machine from the vCenter, and then retry the restore operation. In the **vSphere Client**, the vProxy lock appears as a custom attribute with the name `Dell EMC vProxy Session`.

NOTE: If this attribute contains any value after a vProxyd process failure, backup and restore operations on this virtual machine cannot be performed. Clean up of this attribute and then running a successful restore operation is a requirement in order to avoid any potential data loss or corruption of the virtual machine, otherwise subsequent backups might also contain corrupted data.

DD NFS share not removed after restore to original

The NFS share might not be removed after a successful virtual machine restore to original. When this occurs, the restore hangs and the following NFS clients appear enabled in the DD system.

```
/data/coll/CDM-PP4VM-SD/vProxy-vm-ga-0187.sxi.lab.emc.com-58e24edf-1720-4d00-a530-da6454a3a1b 10.25.11.191 (sec=sys,rw,no_root_squash,no_all_squash,secure,nolock)
/data/coll/CDM-PP4VM-SD/vProxy-vm-ga-0187.sxi.lab.emc.com-58e24edf-1720-4d00-a530-da6454a3a1b 10.6.249.100 (sec=sys,rw,no_root_squash,no_all_squash,secure,nolock)
/data/coll/CDM-PP4VM-SD/vProxy-vm-ga-0187.sxi.lab.emc.com-58e24edf-1720-4d00-a530-da6454a3a1b 10.6.249.140 (sec=sys,rw,no_root_squash,no_all_squash,secure,nolock)
/data/coll/CDM-PP4VM-SD/vProxy-vm-ga-0187.sxi.lab.emc.com-58e24edf-1720-4d00-a530-da6454a3a1b fe80::2501:6dfe:fe6d:eb83 (sec=sys,rw,no_root_squash,no_all_squash,secure,nolock)
/data/coll/CDM-PP4VM-SD/vProxy-vm-ga-0187.sxi.lab.emc.com-58e24edf-1720-4d00-a530-da6454a3a1b fe80::12d7:dff:fe07:d927 (sec=sys,rw,no_root_squash,no_all_squash,secure,nolock)
```

Figure 16. DD NFS clients still enabled after restore

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-ga-xxxxx DDNFS datastore that is mounted on the ESXi host.

IP address change required after successful image-level restore to a new virtual machine

After performing a successful image-level restore to a new virtual machine, ensure that you change the IP address immediately in order to avoid IP conflicts with the original virtual machine. If you do not change the IP to a unique value, subsequent data protection operations might fail on the restored virtual machine, even if that virtual machine's network interfaces are disconnected.

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.

Virtual machine restore fails with name resolution error

A virtual machine restore might fail with the following error due to network issues between protection storage 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 protection storage and PowerProtect Data Manager /vCenter/ESX.

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`.

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 "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 Administrator or Restore Administrator role.

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.

VMware knowledge base articles and product documentation

Additional VMware troubleshooting information is available at the [VMware Knowledge Base](#) and [VMware Documentation](#) websites.

Troubleshooting vSphere Plugin deployments

When investigating issues with the vSphere Plugin deployments, you might need to troubleshoot its deployment.

Troubleshoot vSphere Plugin deployments


In some circumstances, issues can occur during the deployment of the PowerProtect Data Manager **vSphere Plugin**.

About this task

If deployment of the **vSphere Plugin** fails, the plugin displays SSL errors or other errors such as 503 `Service Not Available` or `No Healthy Upstream`, or you need to force the removal and re-installation of the plugin, perform the following steps:

Steps

1. In the PowerProtect Data Manager UI, go to **Infrastructure > Asset Sources**.
2. Select the vCenter asset source, and then click **Edit**.
3. Unselect **vSphere Plugin**, and then click **Save**.
4. Log in to the vCenter mob, for example, `http://vcenter.example.com/mob`.
5. Navigate to a new window to unregister the extension, for example, `http://vcenter.example.com/mob/?moid=ExtensionManager&method=unregisterExtension`
6. On this window, type '`com.emc.dpss.ppdms.plugin`', and then click **Invoke Method**.
7. In the PowerProtect Data Manager UI, go to **Infrastructure > Asset Sources**, select the vCenter, and click **Edit**.
8. Select **vSphere Plugin**, and then click **Save**.
9. Log out of the vCenter Server, and then log back into the vCenter.

 **NOTE:** If this is a newer vCenter server, a blue bar displays with a Refresh button. Click **Refresh**.

VMware knowledge base articles and product documentation

Additional VMware troubleshooting information is available at the [VMware Knowledge Base](#) and [VMware Documentation](#) websites.