PowerProtect Data Manager 19.12

File System User Guide

October 2022
Rev. 01

Notes, cautions, and warnings

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

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

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

Contents

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.

Product naming

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.

Language use

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

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

Acronyms

The acronyms used in this document might not be familiar to everyone. Although most acronyms are defined on their first use, a definition is not always provided with later uses of the acronym. For a list of all acronyms and their definitions, see the glossary at the end of the document.

Website links

The website links used in this document were valid at publication time. If you find a broken link, provide feedback on the document, and a Dell Technologies employee will update the link in the next release as necessary.

Purpose

This document describes how to configure and administer the Dell PowerProtect Data Manager to protect and recover data on the file system host. The *PowerProtect Data Manager Administration and User Guide* provides additional details about configuration and usage procedures.

Audience

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

Revision history

The following table presents the revision history of this document.

Table 1. Revision history

Revision	Date	Description
01	October 25, 2022	Initial release of this document for PowerProtect Data Manager version 19.12.

Compatibility information

Software compatibility information for the PowerProtect Data Manager software is provided by the E-Lab Navigator.

Related documentation

The following publications are available at Customer Support and provide additional information:

Table 2. Related documentation

Title	Content
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 about new features, known limitations, environment, and system requirements for the software.
PowerProtect Data Manager Security Configuration Guide	Contains security information.
PowerProtect Data Manager Amazon Web Services 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 Google Cloud Platform 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 Disaster Recovery (Cloud DR), protect virtual machines in the AWS or Azure cloud, and run recovery operations.
PowerProtect Data Manager Cyber Recovery User Guide	Describes how to install, update, patch, and uninstall the PowerProtect Cyber Recovery software.
PowerProtect Data Manager File System User Guide	Describes how to configure and use the software with the File System agent for file-system data protection.
PowerProtect Data Manager Kubernetes User Guide	Describes how to configure and use the software to back up and restore namespaces and PVCs in a Kubernetes cluster.
PowerProtect Data Manager Microsoft Exchange Server User Guide	Describes how to configure and use the software to back up and restore the data in a Microsoft Exchange Server environment.
PowerProtect Data Manager Microsoft SQL Server User Guide	Describes how to configure and use the software to back up and restore the data in a Microsoft SQL Server environment.
PowerProtect Data Manager Oracle RMAN User Guide	Describes how to configure and use the software to back up and restore the data in an Oracle Server environment.
PowerProtect Data Manager SAP HANA User Guide	Describes how to configure and use the software to back up and restore the data in an SAP HANA Server environment.
PowerProtect Data Manager Storage Direct 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.

Table 2. Related documentation (continued)

Title	Content
PowerProtect Data Manager 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 Virtual Machine User Guide	Describes how to configure and use the software to back up and restore virtual machines and virtual machine disks (VMDKs) in a vCenter Server environment.
VMware Cloud Foundation Disaster Recovery With PowerProtect Data Manager	Provides a detailed description of how to perform an end-to-end disaster recovery of a VMware Cloud Foundation (VCF) environment.
PowerProtect Data Manager Public REST API documentation	Contains the Dell Technologies APIs and includes tutorials to guide you in their use.
vRealize Automation Data Protection Extension for Data Protection Systems Installation and Administration Guide	Describes how to install, configure, and use the vRealize Data Protection Extension.

Typographical conventions

The following type style conventions are used in this document:

Table 3. Style conventions

Formatting	Description
Bold	Used for interface elements that a user specifically selects or clicks, for example, names of buttons, fields, tab names, and menu paths. Also used for the name of a dialog box, page, pane, screen area with title, table label, and window.
Italic	Used for full titles of publications that are referenced in text.
`Monospace`	Used for: ● System code ● System output, such as an error message or script ● Pathnames, file names, file name extensions, prompts, and syntax ● Commands and options
`Monospace italic`	Used for variables.
`Monospace bold`	Used for user input.
[ ]	Square brackets enclose optional values.
|	Vertical line indicates alternate selections. The vertical line means or for the alternate selections.
{ }	Braces enclose content that the user must specify, such as x, y, or z.
...	Ellipses indicate non-essential information that is omitted from the example.

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

Where to find product documentation

- The Customer Support website
- The Community Network
- The PowerProtect Data Manager Info Hub

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.

Support Library

The Support Library contains a knowledge base of applicable solutions that you can search for either by solution number (for example, KB000xxxxxx) or by keyword.

To search the Support Library:

1. Go to the Customer Support website.
2. On the **Support** tab, click **Support Library**.
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 DPADDocFeedback@dell.com.

1

PowerProtect Data Manager File System Agent Overview

Topics:

PowerProtect Data Manager overview

Use PowerProtect Data Manager with the application agent to perform the following operations:

- Automate the configuration of the application agent backup policy and protection storage settings.
- Create a catalog of backups that the application agent creates. Then, monitor that catalog data to determine if retention policies are being adhered to.
- Manage the life cycle of backups that the application agent creates. Ensure that the backups are marked for garbage collection, based on the rules of the retention policy.

PowerProtect Data Manager does not change the way that the application agent works. DBAs, system administrators, or backup administrators create the backups and perform the restore operations.

Introducing the File System agent

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

You can install the File System agent on AIX, Linux, or Windows. See Enabling the File System Agent.

NOTE:

PowerProtect Data Manager supports the coexistence of the Microsoft application agent and the File System agent on Windows. When a volume includes any application database and log files:

- File System agent block-based backups of the volume automatically exclude the database and log files from the file system backup.
- File System agent file-based backups of the volume do not automatically exclude the database and log files, but you can explicitly exclude those files through the exclusion filters in the policy. It is recommended that you exclude the application database and log files from file system backups if you use the corresponding application agent to back up the files.

In both cases, File System agent backups do not involve any database writer, regardless of whether or not the database and log files are excluded. The backups do not interfere with the database backup chaining.

To enable the discovery and scheduling of backups with PowerProtect Data Manager, you must approve the client in the PowerProtect Data Manager UI. Manage the File System agent provides more information.

Software compatibility information for the PowerProtect Data Manager software and application agents is provided by the E-Lab Navigator.

Prerequisites

Ensure that your environment meets the requirements for a new deployment or update of PowerProtect Data Manager.

Requirements:

> **NOTE:** The most up-to-date software compatibility information for the PowerProtect Data Manager software and the application agents is provided by the E-Lab Navigator.

- A list of hosts that write backups to DD systems is available.
- DDOS version 6.1 or later and the PowerProtect DD Management Center are required. All models of DD systems are supported.

  > **NOTE:** PowerProtect DD Management Center is required with a DDOS version earlier than 6.1.2. With DDOS version 6.1.2 or later, you can add and use a DD system directly without PowerProtect DD Management Center.
- Application agent 19.12 or earlier is required.
- License: A trial license is provided with the PowerProtect Data Manager software. Contact Customer Support for assistance with a permanent PowerProtect Data Manager license.
- Large environments require multiple PowerProtect Data Manager instances. Contact Champions.eCDM@emc.com for assistance with sizing requests.
- The PowerProtect Data Manager 19.12 download file requires the following:
  - ESXi version 6.5, 6.7, or 7.0.
  - 10 vCPUs, 24 GB RAM, one 100 GB disk, and one 500 GB disk.
  - The latest version of the Google Chrome browser to access the PowerProtect Data Manager UI.
  - TCP port 7000 is open between PowerProtect Data Manager and the application agent hosts.
- VMware ESXi server that hosts PowerProtect Data Manager meets the following minimum system requirements:
  - 10 CPU cores
  - 24 GB of RAM for PowerProtect Data Manager
  - Five disks with the following capacities:
    - Disk 1—100 GB
    - Disk 2—500 GB
    - Disk 3—10 GB
    - Disk 4—10 GB
    - Disk 5—5 GB
  - One 1-GB NIC

Supported Internet Protocol versions

PowerProtect Data Manager and its components support IPv4 and IPv6 addresses in certain configurations.

Table 4. Supported configurations

Component	Internet Protocol
PowerProtect Data Manager core	IPv4 only or both IPv4 and IPv6
VM Direct and Search	IPv4 only or IPv6 only **NOTE:** Virtual machines that are backed up must use the same protocol that VM Direct uses. Virtual machines can use both IPv4 and IPv6, even though VM Direct cannot.
Application agents integrated with PowerProtect Data Manager:	**NOTE:** If both IPv4 and IPv6 are configured and the PowerProtect Data Manager FQDN is used, the agent uses IPv6 for network communication.
● File System	IPv4, IPv6, or both
● Microsoft Exchange Server	IPv4 only or both IPv4 and IPv6

Table 4. Supported configurations (continued)

Component	Internet Protocol
• Microsoft SQL Server (Application Direct)	IPv4, IPv6, or both
• Microsoft SQL Server (VM Direct)	IPv4 only or IPv6 only **NOTE:** Only the Microsoft SQL Server agent supports VM Direct.
• Oracle RMAN	IPv4, IPv6, or both
• SAP HANA	IPv4, IPv6, or both
• Storage Direct	IPv4 only
Standalone application agents	IPv4 only
Network-attached storage (NAS)	IPv4 only
Kubernetes	IPv4 only
PowerProtect Data Manager management	IPv4 or IPv6
PowerProtect DD communication	IPv4 or IPv6
Report Browser	IPv4 only
SupportAssist	IPv4, IPv6, or both
Syslog Log Server Gateway	IPv4 or IPv6

The following limitations and considerations apply.

Communication with components

If PowerProtect Data Manager is configured to only use one protocol, all components it communicates with must also use that protocol. If some components that PowerProtect Data Manager communicates with use IPv4 and others use IPv6, PowerProtect Data Manager must be configured to use both IPv4 and IPv6.

DD systems and DDVE

If a DD system or a DDVE instance uses only IPv6, the required IPv6 interface must be manually selected when a protection policy is added or edited.

Disaster recovery

Recovering a PowerProtect Data Manager server might result in a conflict with protection-policy configurations. For instance, if the recovered server is configured to use only IPv4, a protection policy that is configured to use IPv6 cannot run.

Name resolution

Name resolution and reverse IP lookup must be configured to ensure the following:

- Fully qualified domain names of PowerProtect Data Manager, its components, and DD components resolve to a valid IPv4 or IPv6 address.
- If both IPv4 and IPv6 addresses are used for DD, both addresses resolve to the same FQDN.
- All IPv4 and IPv6 addresses are valid and reachable.

Server updates

IPv6 is only supported with new installations. Using IPv6 after updating from PowerProtect Data Manager 19.11 or earlier is unsupported.

Storage Policy Based Management

If using vCenter or ESXi 7.0u2 or earlier with only IPv6, SPBM providers must be added using their PowerProtect Data Manager FQDN.

`Service Unavailable` messages with the vSphere Client PowerProtect plug-in

If vCenter uses the vSphere Client PowerProtect plug-in with IPv6 and the vCenter host is added to PowerProtect Data Manager using its IPv6 address or FQDN, `Service Unavailable` messages might be seen for the protected virtual machine. Backups and restores of the protected virtual machine are unaffected, and these messages can be ignored.

Uncompressed IPv6 formatting

Network interfaces that exist on a DD 7.4.x or earlier system and that are configured to use an uncompressed IPv6 format cannot be discovered. An example of an uncompressed IPv6 format is `2620:0000:0170:0597:0000:0000:0001:001a`. An example of a compressed IPv6 format is `2620:0:170:597::1:1a`. To use these network interfaces, reconfigure them to use either an IPv4 address or a compressed IPv6 address, and then initiate a discovery.

Firewall and port considerations

The latest version of the *PowerProtect Data Manager Security Configuration Guide* provides more details about the port requirements.

Table 5. PowerProtect Data Manager port requirements

Description	Communication	Port
SSH communications	Bi-directional communication between the SSH client and the PowerProtect Data Manager appliance.	22 TCP/UDP
Microsoft SQL Server, Oracle, Microsoft Exchange Server, SAP HANA, File System	Bi-directional communication between the PowerProtect Data Manager agent and the PowerProtect Data Manager appliance. Requirement applies to Application Direct and VM Direct.	7000 TCP
REST Server	Bi-directional communication between the HTTP client and the PowerProtect Data Manager appliance.	8443 TCP
RESTAPI Server - VM Direct	Bi-directional communication between the PowerProtect Data Manager agent and the PowerProtect Data Manager appliance. Requirement applies to Microsoft SQL Server VM application-aware.	8443 TCP
UI redirect	Inbound only.	80 TCP 443
LDAP	Outbound only.	389 TCP/UDP 636 TCP

Table 5. PowerProtect Data Manager port requirements (continued)

Description	Communication	Port
Discovery (devices)	Outbound between the PowerProtect Data Manager appliance and the device.	3009 TCP—Storage Direct and DD system 5989 TCP—SMI-S 443 TCP—XtremIO 7225 TCP—RecoverPoint
PowerProtect Data Manager agent	Bi-directional communication between the database hosts and the PowerProtect Data Manager appliance. This requirement applies to both Application Direct and VM Direct.	7000 TCP
Embedded VM Direct service	Outbound.	9090 TCP

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.

Data-in-flight encryption

PowerProtect Data Manager provides centralized management of backup and restore encryption for application agents. Backup and restore encryption is supported for both centralized and self-service operations where applicable.

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. This prevents another party from intercepting private data.

PowerProtect Data Manager only supports encryption in-flight for File System, Kubernetes clusters, Microsoft SQL Server, Microsoft Exchange Server, network attached storage (NAS), Oracle, and SAP HANA workloads. This is a global setting that is applicable to all supported workloads.

For File System, Microsoft SQL Server, Microsoft Exchange Server, Oracle, SAP HANA, and NAS workloads, backup and restore encryption is only supported for Application Direct hosts. For File System agents, restore encryption is supported for image-level restore only. For Microsoft SQL Server agents, restore encryption is supported for database-level restore only.

The *PowerProtect Data Manager Administration and User Guide* and *PowerProtect Data Manager Security Configuration Guide* provide more information about encryption in-flight, such as how to enable the feature and important considerations to understand before enabling.

PowerProtect Data Manager new deployment overview

Familiarize yourself with the high-level steps required to install PowerProtect Data Manager with the File System agent.

Steps

1. Design how to group the backups based on the storage requirements and retention policies.

The account team can help with backup storage design.

2. Install PowerProtect DD Management Center (DDMC).

   PowerProtect Data Manager uses DDMC to connect to the DD systems. The *DD Management Center Installation and Administration Guide* provides instructions.
3. Install PowerProtect Data Manager from the download file.

   The *PowerProtect Data Manager Deployment Guide* provides instructions.
4. Add external DD systems or DDMC to PowerProtect Data Manager.

   The *PowerProtect Data Manager Administration and User Guide* provides instructions on how to add protection storage.
5. Install the File System agent on the appropriate hosts and connect them to PowerProtect Data Manager according to the instructions in the next chapter.
6. Add new or approve pending agent requests in the PowerProtect Data Manager according to the instructions in the next chapter.
7. Add a protection policy for groups of assets that you want to back up.

   ⓘ **NOTE:** After you create a centralized protection job, the first backup is a full backup.

   The *PowerProtect Data Manager Administration and User Guide* provides instructions.
8. Add Service Level Objectives to the protection policy to verify that the protected assets meet the service-level agreements (SLAs).

   The *PowerProtect Data Manager Administration and User Guide* provides instructions.
9. Now that the configuration is complete, it is recommended to perform a full backup so that PowerProtect Data Manager can detect the proper backup chain.

   Without a full backup, PowerProtect Data Manager treats the backups as partial and assumes that you are out of compliance.
10. Monitor protection compliance in the PowerProtect Data Manager dashboard.

PowerProtect Data Manager existing deployment overview

Familiarize yourself with the high-level steps required to install PowerProtect Data Manager with the File System agent in an existing environment.

Steps

1. Install PowerProtect DD Management Center (DDMC).

   PowerProtect Data Manager uses DDMC to connect to the DD systems. The *DD Management Center Installation and Administration Guide* provides instructions.
2. Install PowerProtect Data Manager from the download file.

   The *PowerProtect Data Manager Deployment Guide* provides instructions.
3. Add external DD systems or DDMC to PowerProtect Data Manager.

   The *PowerProtect Data Manager Administration and User Guide* provides instructions on how to add protection storage.
4. Update the File System agent, or uninstall and then reinstall the agent on the hosts, and connect them to PowerProtect Data Manager according to the instructions in the next chapter.
5. Add new or approve pending agent requests in the PowerProtect Data Manager according to the instructions in the next chapter.
6. Add a protection policy for groups of assets that you want to back up.

   ⓘ **NOTE:** After you create a centralized protection job, the first backup is a full backup.

   The *PowerProtect Data Manager Administration and User Guide* provides instructions.
7. Add Service Level Objectives to the protection policy to verify that the protected assets meet the Service Level Agreements (SLAs).

   The *PowerProtect Data Manager Administration and User Guide* provides instructions.

8. Now that the configuration is complete, it is recommended to perform a full backup so that PowerProtect Data Manager can detect the proper backup chain.

   Without a full backup, PowerProtect Data Manager treats the backups as partial and assumes that you are out of compliance.
9. Monitor protection compliance in the PowerProtect Data Manager dashboard.

2

Enabling the File System Agent

Topics:

About the File System agent

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

You can install the File System agent on the host that you plan to protect by using the installation wizard. Installing and uninstalling the File System agent on AIX, Installing and updating the File System agent on Linux, and Installing and updating the File System agent on Windows provide instructions.

Software compatibility information for the PowerProtect Data Manager software and the File System agent is provided in the E-Lab Navigator.

Application agent and File System agent coexistence

PowerProtect Data Manager supports the following application agent and File System agent coexistence:

- Coexistence of the Oracle RMAN agent or SAP HANA agent with the File System agent on Linux.
- Coexistence of the Oracle RMAN agent with the File System agent on AIX.
- Coexistence of the Microsoft SQL Server or Microsoft Exchange Server application agent with the File System agent on Windows.

  ⓘ **NOTE:** When the Microsoft Exchange Server application agent and the File System agent coexist and both agents are installed and registered to the same PowerProtect Data Manager instance, the following workflows are supported.

  For File Systems:

  - Use File-based backup (FBB) instead of Block-based backup, and provide a dummy exclusion filter in the protection policy.
  - In the File System protection policy backup, do not include Microsoft Exchange Server.edb and log file assets.

  For Microsoft Exchange Server:

  - Run Microsoft Exchange Server full backups only.

The coexistence of these agents enables you to protect the Microsoft SQL Server, Microsoft Exchange Server, Oracle, or SAP HANA database with the host file system. The following configurations are supported for agent coexistence:

- Both agents in managed mode (registered to PowerProtect Data Manager)
- The Microsoft SQL Server, Microsoft Exchange Server, Oracle, or SAP HANA agent in stand-alone mode, with the File System agent registered to PowerProtect Data Manager

NOTE: The latest version of each agent must be installed if the agents are registered to PowerProtect Data Manager. The File System agent is supported in managed mode only.

The steps for installation and usage for each agent are the same.

The table below lists the supported use cases and limitations.

Table 6. Supported cases

Category	Supported cases	Current limitations
Agent installation and uninstallation	● New installation of both agents is supported with: ○ Microsoft SQL Server agent, Microsoft Exchange Server agent, Oracle RMAN agent, or SAP HANA agent in stand-alone or managed mode. ○ File System agent in managed mode. ● New installation of an agent is supported in managed mode with an existing agent in stand-alone mode. ● New installation of an agent is supported in stand-alone mode with an existing agent in managed mode. ● Repair of an existing agent installation is supported. ● Uninstallation of agents is supported.	● Uninstalling the last agent that is installed on the host unregisters the host from PowerProtect Data Manager. Any new agent installation that occurs after the uninstall must be newly registered to the PowerProtect Data Manager server. ● Similar to the agent installations, uninstallation of each agent is performed separately.
Host registration and unregistration	● Registration of an installed agent to the PowerProtect Data Manager server is supported. ● Unregistration of agents from the PowerProtect Data Manager server is supported.	● Both agents, if operating in managed mode, should be registered to the same PowerProtect Data Manager server only. There is no option to register each agent to a different PowerProtect Data Manager server. ● Unregistering a host unregisters all the managed agents that are installed on that host. Stand-alone agents are not affected. ● After unregistering a host, the host's assets still appear in the UI in order to support the restore of these assets to a different host. However, backups are not initiated on these assets as the protection policies are disabled.
Backup and restore features	● Protection policy creation is supported on all registered agents. ● All scheduled protection policy backups are supported on both agents as per individual protection policies. ● Self-service backups are supported on both agents. ● Compliance is supported on both agents as per the individual service-level agreements (SLAs). ● Manual backups are supported at the protection policy level and individual asset level through the centralized protection policy workflow.	

File System agent prerequisites

Review the following prerequisites before installing and using the File System agent in PowerProtect Data Manager.

Windows, Linux, and AIX prerequisites

- Ensure that your host is a 64-bit system. PowerProtect Data Manager supports only 64-bit hosts.
- Ensure that your host is a supported operating system version. Software compatibility information for the PowerProtect Data Manager software is provided in the E-Lab Navigator.
- Ensure that all clocks on both the host and PowerProtect Data Manager are time-synced to the local NTP server to ensure discovery of the backups.
- Ensure that the host and the PowerProtect Data Manager network can see and resolve each other. If PowerProtect Data Manager and the File System agent are registered in different domains, you must add IP address and Fully Qualified Domain Name (FQDN) entries on both the client and server.
    1. Browse to the path of the hosts file. For example, on Windows `C:\Windows\System32\drivers\etc\hosts`, and on Linux `/etc/hosts`.
    2. Add an entry to the hosts file, as in the following:

```
IP address     FQDN            common name
10.10.100.100  yourdomain.com  yourdomain
```

- LVM and VxVM partitions or volumes are supported.
- Physical partitions are supported only when using file-based backups.
- Each volume group on LVM2 or VxVM must have at least 10% free space for a block-based backup to succeed. For successful Windows VSS snapshot during block-based or file-based backup, the free space requirement is 20%.
- For file-based backups, ensure that the drive on which the File System agent is installed has adequate free space for the metadata record files that are created during a backup. Provide about 250 MB free space for each million files that you are backing up.
- For any ESXi version 6.5 or earlier host with PowerStore storage attached, the Windows operating system deployment or installation cannot proceed. If the *DiskMaxIOSize* parameter is not configured with the proper value, the File System agent backup and restore operations fail. Ensure that you set the *DiskMaxIOSize* to 1024 KB.
- Ensure that no service is using port 7010 or 7011. These ports must be reserved for File System agent operations.
- Review the limitations in the section File System agent limitations.

Additional Linux prerequisites

- File system discovery requires an ext3, ext4, XFS, or BTRFS file system type.
- On the Linux hosts that have the UEFI Secure Boot option enabled, block-based backup drivers do not load, and the error message `insmod: ERROR: could not insert module /lib/ modules/ 3.10.0-693.el7.x86_64/ extra/nsrbbb.ko: Required key not available` appears. As a workaround, you can disable the Secure Boot option.
- Ensure that the file system has the `/etc/fstab` entry. Without the `/etc/fstab` entry, discovery fails.
- To enable file-level restores, complete the following:
    1. Log in to the system you are restoring from as **`root`**.
    2. Install iSCSI client packages.

       See the Operating System documentation for the installation procedure.
    3. For **Service Start**, choose **Manually**, and then click **OK**.
- If installing the block-based backup driver, review the output of the `cat /proc/sys/kernel/kptr_restrict` file to verify that permissions to install the driver are set. If the value is set to **2**, then there is a restriction that might result in block-based backup driver installation failure. Run the following command to change this setting:

```
echo 1 > /proc/sys/kernel/kptr_restrict
```

- Install the lsb_release package.

  See the Operating System documentation for the installation procedure.

Additional AIX prerequisites

- File system discovery requires a JFS or JFS2 file system type.
- Ensure that IBM XL C or C++ Runtime for AIX 16.1.0.7 and later is installed.

File System agent limitations

Review the following limitations that are related to File System agent support in PowerProtect Data Manager.

Software compatibility

Software compatibility information for the PowerProtect Data Manager software and the File System agent is provided in the E-Lab Navigator.

Windows and Linux limitations

- File System agent block-based backups exclude the following:
  - Application files such as Microsoft SQL Server and Microsoft Exchange Server files.

    > **NOTE:** For file-based backups, application data such as Microsoft SQL Server and Microsoft Exchange Server data is backed up, but you can explicitly exclude the data through the exclusion filters in the policy. It is recommended that you exclude the application data from file system backups if you use the corresponding application agent to back up the data. File System agent backups do not involve any database writer, regardless of whether or not the application data is excluded. The backups do not interfere with the database backup chaining.

  - HyperVisor files. You cannot run a Hyper-V server in a VMware virtual machine.
  - Data belonging to individual application writers.
  - Unsupported application writer files.
- It is recommended to use different mount points for each drive. Reusing mount points might cause unexpected issues during file system discovery.
- The File System agent supports operating systems in only the following languages:
  - English — full support.
  - Japanese — the File System agent can be used for all protection and restore operations on a Japanese-language operating system, provided that volume asset names are in English. Only file and folder names can be in Japanese.
- If a Windows or Linux file system host is unregistered from PowerProtect Data Manager and then re-registered with a different FQDN, because PowerProtect Data Manager recognizes the registration as a new host by its new name, duplicate asset entries appear in the UI—those for the host that is registered earlier, as well as for the host that is registered by the new name. This does not impact backup and restore functionality on the new host.
- The File System agent and application agents use the FQDN for registration. If the File System agent coexists with the Microsoft SQL, Oracle, or SAP HANA application agent, both agents must use the FQDN.
- For a protection policy backup with assets from different hosts, the backup status appears as *Failed* in the UI if the backup of one asset within the policy fails.
- Running the `ddfssv` and `ddfsrc` commands to perform self-service backup and restore of file systems fails if you provide the DD hostname (instead of IP) for the *DFA_SI_DD_HOST* variable.
- If the Bytes of sector sizes of the source and target volumes are different, PowerProtect Data Manager does not support block-based image recoveries. For example, you cannot perform a block-based image recovery of a volume that has 4096 as the Bytes of sector size to a volume that has 512 as the Bytes of sector size, and vice versa.

Windows Limitations

- The file-level restore of a folder can result in the loss of the sparse flag of any sparse files within the folder. To preserve the sparse flag of these files, restore the files individually.

Linux limitations

- On the Linux hosts that have the UEFI Secure Boot option enabled, block-based backup drivers do not load, and the error message `insmod: ERROR: could not insert module /lib/ modules/ 3.10.0-693.el7.x86_64/ extra/nsrbbb.ko: Required key not available` appears. As a workaround, you can disable the Secure Boot option.
- A file system backup might fail with the error `Insufficient space exists in the volume group for creating shadow of the volume` when there is not enough space in the volume group for a block-based backup to succeed. Each volume group on LVM2 or VxVM must have at least 10% free space.
- On Linux, performing an image-level restore of a block-based backup volume to an alternate location changes the GUID for the volume. As a result, PowerProtect Data Manager displays duplicate assets on the **Infrastructure** > **Assets** pane, where the older asset has a status of **Deleted** or **Not Detected**. To ensure continued protection, replace the old asset in the protection policy with the new asset.

AIX limitations

- On AIX, PowerProtect Data Manager supports only file-based backups. Block-based backups are not supported.

Block-based backups

Block-based backups provide instant access to the backups. The block-based backups enable you to mount the backups by using the same file systems that you used to back up the data.

The File System agent's block-based backups support the following capabilities:

- Mounting of a backup as a file system
- Mounting of an incremental backup
- Sparse backup support
- Backups of operating system-deduplicated file systems as source volumes on Windows
- Forever virtual full backups to DD
- DD retention lock
- Recoveries from DD

Block-based backups are useful for datasets that are under 10 TB with a single volume under 5 TB, and a daily change rate under 5%.

Best practices for file system backups

Consider the following best practices for file system backups.

- Ensure that subsequent backup schedules do not overlap.

  If a full backup is in progress when the next incremental backup starts, then the incremental backup is promoted to a full backup. If the schedules overlap, the incremental backup continues to get promoted to a full backup because a full backup has not completed. Also, overlapping backup schedules might fail as a result of concurrent snapshots or other limitations that are caused by the underlying system.

  To identify the optimal backup window between full backups and the first incremental backup, measure the backup time that is required for a small asset. Use this time as an indicator to assess the backup window for assets that are larger in size. For example:

  - Data backup speed = asset size / time taken to back up the asset
  - Total backup size = sum of the total size of the assets to be backed up for a full backup
  - Maximum backup window = total backup size / data backup speed
  - Optimal backup window = maximum backup window / parallelism value
- If the data source is encrypted or compressed, the DD system provides limited deduplication. This increases the time that is taken to back up the data, as compared to data that is not encrypted or compressed.

Configure the file system parallel backup setting

PowerProtect Data Manager enables you to run file system backups in parallel to reduce the time taken for backups. This setting defines the maximum concurrent network sessions from the client to the DD system at any given time. You can specify the number of streams to use for the backup in the configuration file `.ddfssv.fsagentconfig` or through the self-service CLI. However, it is recommended that you set the parallelism value in the configuration file as the parallelism value provided in the configuration file takes precedence over the parallelism value that is provided in the CLI.

> **NOTE:** Backup parallelism is only available on supported Windows systems. Since the parallelism setting is defined at the host level, you must set the parallelism setting on every Windows host where parallel file system backups are enabled.

To specify the number of streams to use for the backup, you can set the file system parameter `--max-host-streams` in the `.ddfssv.fsagentconfig` file that is located in the `C:\Program Files\DPSAPPS\fsagent\settings` directory on the file system host. This value must be an integer. The default value is `8`.

For example, if you set the `--max-host-streams` parameter value to 6, the File System agent backups run with 6 streams:

```
--max-host-streams=6
```

You can also use the command-line option `-M` to specify the number of streams to use for the backup. For example:

```
ddfssv -LL -l INCR -z -M 4 -a DFA_SI=TRUE
-a DFA_SI_USE_DD=TRUE -a DFA_SI_DD_HOST=protection_storage_system_ip_address
-a DFA_SI_DD_USER=protection_storage_user -a
DFA_SI_DD_PASSWORD=protection_storage_system_password -a
DFA_SI_DEVICE_PATH=protection_storage_device_path I:
```

where:

-a "DFA_SI_DD_HOST=*protection_storage_system_ip_address*"

Specifies the name of the DD server that contains the storage unit where you want to back up the databases.

-a "DFA_SI_DD_PASSWORD=*protection_storage_system_password*"

Specifies the password of the protection storage system user.

-a "DFA_SI_DEVICE_PATH=*protection_storage_device_path*"

Specifies the name and the path of the protection storage device where you want to direct the backup.

-a "DFA_SI_DD_USER=*protection_storage_user*"

Specifies the protection storage username. For example, sysadmin.

Recommendations for optimal performance:

- Tune the parallelism value based on the resources that are available on your system, including the CPU, the number of assets, and the connection bandwidth to the DD system.
- Set the parallelism value equal to the number of CPU cores on the host.
- Run backups in parallel for several assets that are small in size, as opposed to running backups in parallel for a few assets that are large in size.

Configure asset multi-streaming for file-based backups

PowerProtect Data Manager supports *asset multi-streaming*, which enables you to run a file system backup of an asset in parallel streams to reduce the time required to complete the file-based backup. Asset multi-streaming is enabled by default.

When using asset multi-streaming for file-based backups of large volumes, the contents of the volumes are divided into chunks. These chunks are backed up in parallel in multiple streams to increase the backup throughput.

The chunk size is a configurable parameter, with a default value of 50 GB (`--chunkersize=50`). The number of parallel streams is set by the `--max-host-streams` parameter in the configuration file, or the `-M` command-line option, as described in Configure the file system parallel backup setting. The value for number of parallel streams set in the config file takes precedence over the value set in the CLI. The number of streams is set per host (and not per asset), and each asset uses the streams available to it.

Creating chunks and multi-streaming the backup consumes some extra computing resources. You can control that usage by tuning the `chunkersize` and `--max-host-streams` parameters. If, after tuning, you are still not satisfied with the resource usage, you can disable multi-streaming. To do so, add the `--disable-asset-multistreaming=true` parameter in the configuration file, `.ddfssv.fsagentconfig` under the `Settings` folder.

Multi-streaming may not yield desired results in the following scenarios:

- System has limited CPUs or memory.
- Reads are slow, in which case, CPU usage will be high. For disks with slow read or high latency, disable multi-streaming.
- You are backing up many small files. Multi-streaming gives better performance when files are large. Many small files can cause undesirably high CPU usage levels.

Recommendations for optimal performance:

- Multi-streaming can be CPU-intensive. It is important to tune the environment for optimal chunk size and an optimal number of streams.
- If there are more volumes than streams in a protection policy, disable asset multi-streaming.

Protect an asset with the File System agent

The following task describes the steps required to protect an asset with a protection policy.

Steps

1. Add a storage system.

   For more information, see the *PowerProtect Data Manager Administration and User Guide*.
2. Install the File System agent on the file system host.

   For more information, see the section on installing the File System agent on the operating system of the host.
3. Add or approve the File System agent on the file system host.

   For more information, see Manage the File System agent.
4. Discover the file system asset.

   For more information, see Discover a file system host.
5. Create a protection policy to protect the file system.

   For more information, see Adding a protection policy for File System protection.

   ⓘ **NOTE:** You cannot perform a backup to a secondary DD system. You can only restore from a secondary DD system.

Protect an asset in a Microsoft Windows Server clustered environment with the File System agent

The following task describes the steps required to protect clustered disks and Cluster Shared Volumes with a protection policy.

About this task

Repeat these steps for each node in the cluster that is registered with PowerProtect Data Manager.

Steps

1. Add a storage system.

   For more information, see the *PowerProtect Data Manager Administration and User Guide*.
2. Install the File System agent on the node.

   For more information, see Install the File System agent on Windows .

   ⓘ **NOTE:** Cluster assets are automatically discovered after the agent is installed.
3. Add or approve the File System agent on the node.

   For more information, see Manage the File System agent.

4. Discover the file system asset.

   For more information, see Discover a file system host.

   NOTE: Stand-alone assets on a node are listed under the name of the cluster node. Cluster assets on a node are listed under the name of the logical cluster host.

5. Create a protection policy to protect the cluster.

   For more information, see Adding a protection policy for File System protection.

   NOTE: The backup of a cluster asset is routed through the node on which the asset or volume is active.

6. If you are planning to use bare-metal recovery for disaster recovery, record the hardware configuration of the cluster-node Windows clients.

   CAUTION: Bare-metal recovery can fail if the hardware configuration of the new Windows clients does not match the hardware configuration of the old cluster-node Windows clients.

   Necessary information includes the hardware vendor, size and type of disks, type of network adapters, and amount of memory assigned.

Installing and uninstalling the File System agent on AIX

Learn how to install and uninstall the File System agent on AIX.

Install the File System agent on AIX

Install the File System agent on supported AIX systems using an interactive or silent installation procedure.

Install the File System agent on AIX in interactive mode

Use this interactive procedure to install the File System agent on supported AIX systems.

Prerequisites

- Ensure that you review the prerequisites provided in File System agent prerequisites.
- Download the File System agent software package to the AIX host.

NOTE: If a value is not provided for *PowerProtect Server IP* in the installation commands, the product is installed without PowerProtect registration, and no backups can be initiated from the UI.

Steps

1. In the PowerProtect Data Manager UI:
   a. Click ⚙, and then select **Downloads** from the **System Settings** menu.
   b. Select the File System agent download package for AIX, `fsagent1912_aixpower72.tar.gz`.
   c. Download the package in the location that you want to install the File System agent.

      NOTE: Relocating the installation to another partition or mount point on AIX is not supported.

2. Untar the installer by running the following commands:
   a. gunzip fsagent1912_aixpower72.tar.gz
   b. tar -xvf fsagent1912_aixpower72.tar
3. To change the current working directory to the extracted path, run the command **`cd fsagent`**.
4. Run the installation script **`install.sh`**.

   To run in debug mode, run **`install.sh --debug`**.

   To get help, run **`install.sh --help`**.

ⓘ **NOTE:** File System agent does not support block-based backups on AIX. All backups performed by File System agent on AIX will be file-based backups.

The following `.rte` files are installed as part of the script:

- `powerprotect-agentsvc.rte` —Installs or updates the agent service component for the File System agent.
- `ppdm_fsagent.rte` —Installs the File System agent related files and folders.

5. Type the PowerProtect Data Manager server FQDN or IP address. It is recommended to use the FQDN.

ⓘ **NOTE:**

- If another application agent is already installed on the client and registered to PowerProtect, ensure that you register the agent with the existing PowerProtect Data Manager server FQDN. When you register the agent with a PowerProtect Data Manager server that is different from the currently registered server, no warning message appears, and requests are routed to the newer server instance.
- If you specify a hostname or fully qualified domain name (FQDN) with an underscore (_) for the PowerProtect Data Manager server, then the communication will be done by the system's IP, if provided to the system on registration.

6. To enable the PowerProtect Data Manager communication 7000 TCP port, run the `/opt/dpsapps/agentsvc/configfw.sh` script as the root user.
The system responds that the firewall script is running, and is configuring firewall rules.

Install the File System agent on AIX in silent mode

On AIX, review the following commands to perform a silent installation of the File System agent.

ⓘ **NOTE:** The `--server` option is used to specify the PowerProtect server IP for registration, and is mandatory for silent install.

Use the following commands to perform a silent installation on AIX:

- For silent installation, including registration of the agent with the PowerProtect server, type: **`install.sh --silent-install --server=<PowerProtect_server_IP>`**
- To run the installer in debug mode during silent installation, type: **`install.sh --debug --silent-install --server=<PowerProtect_server_IP>`**
- To skip installation of the block-based backup driver, type: **`install.sh --skip-driver --silent-install --server=<PowerProtect_server_IP>`**.
- To enable the PowerProtect Data Manager communication 7000 TCP port, run the `/opt/dpsapps/agentsvc/configfw.sh` script as the root user.

Uninstall the File System agent on AIX

On AIX, you can uninstall the File System agent by performing the following steps:

Steps

1. Obtain the `uninstall.sh` script from the folder extracted from the package `fsagent1910_aixpower72.tar.gz` or under `/opt/dpsapps/fsagent/bin`.
2. Run **`./uninstall.sh`**.

   The following message appears:

```
Other application agents might be using powerprotect-agentsvc. Do you wish to
uninstall powerprotect-agentsvc? [y/n]
```

3. To confirm that you want to uninstall `powerprotect-agentsvc`, type **`Y`**.

ⓘ **NOTE:** If you type **`N`**, the .rpm files (`ppdm_bbbwt.rpm` and `ppdm_fsagent.rpm`) and .deb files (`ppdm-bbbwt.deb` and `ppdm-fsagent.deb`) are uninstalled. However, `powerprotect-agentsvc` remains in an installed state.

There is no silent uninstall procedure on AIX.

Installing and updating the File System agent on Linux

Learn how to install and update the File System agent on Linux.

Install the File System agent on Linux

Install the File System agent on supported Linux systems using an interactive or silent installation procedure.

Install the File System agent on Linux in interactive mode

Use this interactive procedure to Install the File System agent on supported Linux systems.

Prerequisites

- Ensure that you review the prerequisites provided in File System agent prerequisites.
- Download the File System agent software package to the Linux host.

> **NOTE:** If a value is not provided for *PowerProtect Server IP* in the installation commands, the product is installed without PowerProtect registration, and no backups can be initiated from the UI.

Steps

1. In the PowerProtect Data Manager UI:

   a. Click ⚙, and then select **Downloads** from the **System Settings** menu.

   b. Select the File System agent download package for Linux, `fsagent1912_linux_x86_64.tar.gz`.

   c. Download the package in the location that you want to install the File System agent.

   > **NOTE:** Relocating the installation to another partition or mount point on Linux is not supported.

2. Untar the installer by running **`tar -xvf fsagent1912_linux_x86_64.tar.gz`**.

   Then, run the command `cd fsagent` to change the current working directory to the extracted path.

   > **NOTE:** To verify the authenticity and integrity of the RPM files prior to the installation step, follow the instructions in the *PowerProtect Data Manager Security Configuration Guide*.

3. Run the installation script **`install.sh`**.

   To run in debug mode, run **`install.sh --debug`**.

   To get help, run **`install.sh --help`**.

   > **NOTE:** For installations on Oracle Linux distributions or CentOS Linux distributions (for CentOS 8.0, 8.1, and 8.2), run **`install.sh --skip-driver`** to skip the block-based backup driver installation. These distributions do not currently support block-based backups. All backups performed by the File System agent on these distributions will be file-based backups.

   For RHEL distributions (for Red Hat 8.0, 8.1, and 8.2), Security-Enhanced Linux (SELinux) is enabled by default. It can support block-based backups, provided you continue the installation with the procedure in Install the File System agent on RHEL distributions.

   The following `.rpm` or `.deb` files are installed as part of the script:

   - `powerprotect-agentsvc.rpm` or `powerprotect-agentsvc.deb`—Installs or updates the agent service component for the File System agent.
   - `ppdm_bbbwt.rpm` or `ppdm-bbbwt.deb`—Installs the block-based backups driver.
   - `ppdm_fsagent.rpm` or `ppdm-fsagent.deb`—Installs the File System agent related files and folders.

4. Type the PowerProtect Data Manager server FQDN or IP address. It is recommended to use the FQDN.

   > **NOTE:**
   >
   > - If another application agent is already installed on the client and registered to PowerProtect, ensure that you register the agent with the existing PowerProtect Data Manager server FQDN. When you register the agent with

a PowerProtect Data Manager server that is different from the currently registered server, no warning message appears, and requests are routed to the newer server instance.

- If you specify a hostname or fully qualified domain name (FQDN) with an underscore (_) for the PowerProtect Data Manager server, then the communication will be done by the system's IP, if provided the system on registration.

5. To enable the PowerProtect Data Manager communication 7000 TCP port, run the `/opt/dpsapps/agentsvc/configfw.sh` script as the root user.
   The system responds that the firewall script is running, and is configuring firewall rules.

   NOTE: If the firewall rules are not applied, restart the firewall.

Next steps

If the host is not already approved, add the file system host to the PowerProtect Data Manager server. Manage the File System agent provides more information.

Discover file system assets. Discover a file system host provides more information.

Install the File System agent on RHEL distributions

For RHEL distributions (for Red Hat 8.0, 8.1, and 8.2), Security-Enhanced Linux (SELinux) is enabled by default. To support block-based backups, run this special installation procedure.

Prerequisites

Complete steps 1 and 2 in Install the File System agent on Linux in interactive mode

Steps

1. If you have not yet run the installation script, **`install.sh`**, run it now.
   Installation of the block-based backup driver fails.
2. Check that an error message similar to the following appears in `/var/log/messages`
   ```
   insmod: ERROR: could not insert module /lib/modules/4.18.0-80.el8.x86_64/extra/nsrbbb.ko:
   Permission denied.
   ```
3. To check the audit log, run: **`ausearch -c 'insmod'`**

   It returns a string similar to:
   ```
   type=AVC msg=audit(1624349147.478:628):
   avc: denied { module_load } for pid=80964
   comm='insmod' path="/opt/dpsapps/fsagent/bin/nsrbbb-redhatenterprise-8.2-4.18.0-193.ko"
   dev="dm-0" ino=12098527 scontext=system_u:system_r:unconfined_service_t:s0
   tcontext=unconfined_u:object_r:bin_t:s0 tclass=system permissive=0
   ```

   `type=AVC` indicates that the installation of the block-based backup driver is failing due to the SELinux policy.
4. To change the SELinux policy so that it will be able to allow access to the block-based backup driver, run: **`ausearch -c 'insmod' --raw | audit2allow -M ppdm-fsagent`**
   It generates two files in the current directory: `ppdm-fsagent.pp` and `ppdm-fsagent.te`
5. To apply the SELinux policy changes, to enable access to the block-based backup driver, run: **`semodule -i ppdm-fsagent.pp`**
6. Run the installation script once again: **`install.sh`**
   Installation of the block-based backup driver should succeed, and the following `.rpm` or `.deb` files are installed as part of the script:
   - `powerprotect-agentsvc.rpm` or `powerprotect-agentsvc.deb`—Installs or updates the agent service component for the File System agent.
   - `ppdm_bbbwt.rpm` or `ppdm-bbbwt.deb`—Installs the block-based backups driver.
   - `ppdm_fsagent.rpm` or `ppdm-fsagent.deb`—Installs the File System agent related files and folders.
7. Type the PowerProtect Data Manager server FQDN or IP address. It is recommended to use the FQDN.

   NOTE: If another application agent is already installed on the client and registered to PowerProtect, ensure that you register the agent with the existing PowerProtect Data Manager server FQDN. When you register the agent with a PowerProtect Data Manager server that is different from the currently registered server, no warning message appears, and requests are routed to the newer server instance.

Next steps

If the host is not already approved, add the file system host to the PowerProtect Data Manager server. Manage the File System agent provides more information.

Discover file system assets. Discover a file system host provides more information.

Install the File System agent on Linux in silent mode

On Linux, review the following commands to perform a silent installation of the File System agent.

> **NOTE:** The `--server` option is used to specify the PowerProtect server IP for registration, and is mandatory for silent install.
>
> To verify the authenticity and integrity of the RPM files prior to the installation step, follow the instructions in the *PowerProtect Data Manager Security Configuration Guide*.

Use the following commands to perform a silent installation on Linux:

- For silent installation, including registration of the agent with the PowerProtect server, type: **`install.sh --silent-install --server=<PowerProtect_server_IP>`**
- To run the installer in debug mode during silent installation, type: **`install.sh --debug --silent-install --server=<PowerProtect_server_IP>`**
- To skip installation of the block-based backup driver, type: **`install.sh --skip-driver --silent-install --server=<PowerProtect_server_IP>`**.
- To enable the PowerProtect Data Manager communication 7000 TCP port, run the `/opt/dpsapps/agentsvc/configfw.sh` script as the root user.

Update the File System agent on Linux

The File System agent supports a direct update from an earlier version if you are using an earlier version of PowerProtect Data Manager. You can update the PowerProtect Data Manager File System agent on supported Linux systems in interactive or silent mode.

Update and register the latest version of the PowerProtect Data Manager File System agent for Linux with the same PowerProtect Data Manager server in the same location.

> **NOTE:**
>
> - When you install or update the File System agent, other app agents on the system must be updated to the same version as the File System agent.
> - Following an update, the first block-based backup is promoted to a full backup.

Update the File System agent on Linux in interactive mode

Use this interactive procedure to update the File System agent on supported Linux systems.

Prerequisites

- Ensure that you review the prerequisites provided in File System agent prerequisites.
- Download the File System agent software package to the Linux host.

Steps

1. In the PowerProtect Data Manager UI:
   a. Click ⚙, and then select **Downloads** from the **System Settings** menu.
   b. Select the File System agent download package for Linux, `fsagent1912_linux_x86_64.tar.gz`.
   c. Download the package in the location that you want to install the File System agent.

      > **NOTE:** Relocating the installation to another partition or mount point on Linux is not supported.

2. Untar the installer by running **`tar xvf fsagent1912_linux_x86_64.tar.gz`**.

Then, run the command `cd fsagent` to change the current working directory to the extracted path.

> **NOTE:** To verify the authenticity and integrity of the RPM files prior to the installation step, follow the instructions in the *PowerProtect Data Manager Security Configuration Guide*.

3. Run the `install.sh` script.
   The following `.rpm` or `.deb` files are installed as part of the script:
   - `powerprotect-agentsvc.rpm` or `powerprotect-agentsvc.deb`—Installs or updates the agent service component for File System agent.
   - `ppdm_bbbwt.rpm` or `ppdm-bbbwt.deb`—Installs the block-based backups driver.
   - `ppdm_fsagent.rpm` or `ppdm-fsagent.deb`—Installs the File System agent related files and folders.
4. Type the PowerProtect Data Manager server FQDN or IP address. It is recommended to use the FQDN.

   > **NOTE:** If another application agent is already installed on the client and registered to PowerProtect, ensure that you register the agent with the existing PowerProtect Data Manager server FQDN. When you register the agent with a PowerProtect Data Manager server that is different from the currently registered server, no warning message appears, and requests are routed to the newer server instance.

5. To enable the PowerProtect Data Manager communication 7000 TCP port, run the `/opt/dpsapps/agentsvc/configfw.sh` script as the root user.
   The system responds that the firewall script is running, and is configuring firewall rules.

   > **NOTE:** If the firewall rules are not applied, restart the firewall.

Update the File System agent on Linux in silent mode

Use the following commands to perform a silent update of the File System agent on Linux:

> **NOTE:** To verify the authenticity and integrity of the RPM files prior to the update step, follow the instructions in the *PowerProtect Data Manager Security Configuration Guide*.

- To run the silent agent update, type: **`install.sh --force-upgrade`**

  > **NOTE:** The `--force-upgrade` command line option does not prompt users to update other agents so that they are running the same version as the File System agent. Ensure that other agents are running the same version as the File System agent; otherwise, those agents will not work.

- To run the silent update and register the agent with a new PowerProtect server, type: **`install.sh --force-upgrade --server=`*`PowerProtect Server IP`***
- For silent update in debugging mode, type: **`install.sh --force-upgrade --debug`**

  > **NOTE:** During silent installation or update, the debug output is directed to syslog to be viewed later.

- To enable the PowerProtect Data Manager communication 7000 TCP port, run the `/opt/dpsapps/agentsvc/configfw.sh` script as the root user.

Uninstall the File System agent on Linux

On Linux, you can uninstall the File System agent by performing the following steps:

Steps

1. Obtain the `uninstall.sh` script from the folder extracted from the package `fsagent1910_linux_x86_64.tar.gz` or under `/opt/dpsapps/fsagent/bin`.
2. Run **`./uninstall.sh`**.

   The following message appears:

   ```
   Other application agents might be using powerprotect-agentsvc. Do you wish to
   uninstall powerprotect-agentsvc? [y/n]
   ```

3. Type **`Y`** to confirm that you want to uninstall `powerprotect-agentsvc`.

NOTE: If you type **`N`**, the .rte files (`ppdm_fsagent.rte`, `ppdm-bbbwt.rte` and `ppdm-fsagent.rte`) are uninstalled. However, `powerprotect-agentsvc` remains in an installed state.

There is no silent uninstall procedure on Linux.

Recommission the File System agent on Linux or AIX

You can use the procedure in this topic to onboard the decommissioned File System agent to the same PowerProtect Data Manager server.

NOTE: You can run the `install.sh` or `register.sh` script to register and recommission the File System agent with PowerProtect Data Manager only if you have not uninstalled the File System agent and PowerProtect agent service.

If you have cleaned up the installation directories and manually uninstalled both the File System agent and PowerProtect agent service, then you must complete the installation procedures in Installing and updating the File System agent on Linux.

To use the `install.sh` script to register and recommission the File System agent with PowerProtect Data Manager, run:

```
install.sh --server=10.125.19.40 --debug
```

The message `AgentService is recommissioned` is displayed to confirm that the agent has been successfully recommissioned.

To use the `register.sh` script to register and recommission the File System agent with PowerProtect Data Manager, run:

```
/opt/dpsapps/agentsvc/register.sh --enable
```

Installing and updating the File System agent on Windows

Learn how to install and update the File System agent on Windows.

Install the File System agent on Windows

Install the File System agent on supported Windows systems using an interactive or silent installation procedure.

NOTE: In a clustered environment, install the same version of the File System agent on each node in the cluster that is registered with PowerProtect Data Manager.

Install the File System agent on Windows in interactive mode

Use this interactive procedure to Install the File System agent on supported Windows systems.

Prerequisites

- Ensure that you carry out the prerequisites provided in File System agent prerequisites.
- Download the File System agent software package.

Steps

1. In the PowerProtect Data Manager UI:
   a. Click ⚙, and then select **Downloads** from the **System Settings** menu.
   b. Select the File System agent download package for Windows, `fsagent1912_win_x64.zip`.
   c. Download the package in the location that you want to install the File System agent.
2. Run the `fsagent-19.12.0.0.exe` program.
3. Follow the wizard installation steps to provide the installation location and the PowerProtect Data Manager server IP address.

ⓘ **NOTE:** If another application agent is already installed on the client and registered to PowerProtect, ensure that you register the agent with the existing PowerProtect Data Manager server IP. When you register the agent with a PowerProtect Data Manager server that is different from the currently registered server, no warning message appears, and requests are routed to the newer server instance.

- If another application agent is already installed on the client and registered to PowerProtect, ensure that you register the agent with the existing PowerProtect Data Manager server IP. When you register the agent with a PowerProtect Data Manager server that is different from the currently registered server, no warning message appears, and requests are routed to the newer server instance.
- If you specify a hostname or fully qualified domain name (FQDN) with an underscore (_) for the PowerProtect Data Manager server, then the communication will be done by the system's IP, if provided the system on registration.

To enable the PowerProtect Data Manager communications port 7000, ensure that the **Configure the Windows Firewall** option is selected under **Common Core Components**. This option is selected by default.

ⓘ **NOTE:**

When the **Configure the Windows Firewall** option is enabled, the installation creates the Windows firewall rule that allows inbound and outbound connections for the agent service process. Installation of the File System agent requires port 7000 on the File System agent host and port 8443 on PowerProtect Data Manager to be open bidirectionally. These ports enable communication between the File System agent and PowerProtect Data Manager.

If the Microsoft application agent is already installed and firewall rules are configured, then the **Configure the Windows Firewall** option is selected by default but disabled for the File System agent.

4. Click **Install**.
   The following `msi` files are used for the installation:
   - `AgentService.msi`—Installs or updates the agent service component for File System agent.
   - `BBBWT.msi`—Installs the block-based backups driver.
   - `Fsagent.msi`—Installs the File System agent related files and folders.
5. Click **Finish**.

   ⓘ **NOTE:** If a change occurred to the PowerProtect Data Manager server IP address, the installation completes successfully but the client registration fails. To re-register the client to the correct IP address, use the **Modify** option under **Add/Remove programs** for the File System agent, and then restart the PowerProtect service agent service on the client.

Next steps

Windows installer logs are retained at `<System drive>\Users\<installing user>\AppData\Local\Temp`, and should be consulted in the event of an installation failure.

If the host is not already approved, add the file system host to the PowerProtect Data Manager server. Manage the File System agent provides more information.

Discover file system assets. Discover a file system host provides more information.

ⓘ **NOTE:** If you change the FQDN of the client at any point, use the **Modify** option under **Add/Remove programs** to update the registration information for the File System agent, and then restart the agent service on the client to reregister the client with the PowerProtect Data Manager server.

Install the File System agent on Windows in silent mode

On Windows, review the following commands to perform a silent installation of the File System agent.

ⓘ **NOTE:** The File System agent installer for Windows does not support the `--help` option. Running the installer program with `--help` initiates the actual installation process.

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

```
fsagent-19.12.0.0.exe /s PPDMHostName=<PPDM_server_IP>
```

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

```
fsagent-19.12.0.0.exe /s PPDMHostName=<PPDM_server_IP>
ProductInstallPath="D:\alternate_path"
```

To enable the PowerProtect Data Manager communications port 7000, if Windows firewall rules have not been previously configured, run:

```
fsagent-19.12.0.0.exe /s PPDMHostName=<PPDM_server_IP> EnableFirewallRules=1
```

When `EnableFirewallRules` is enabled (set to '1'), the installation creates the Windows firewall rules that allows inbound and outbound connections for the agent service process. Installation of the File System agent requires port 7000 on the File System agent host and port 8443 on PowerProtect Data Manager to be open bidirectionally. These ports enable communication between the File System agent and PowerProtect Data Manager.

The change in EnableFirewallRules configuration will take place only on first-time installation or upgrade of the agent service.

In silent File System agent installation (in the case of coexistence), use the `ForceUpgrade=1` option to cause the silent update of common components. If you do not add this option, the silent installation fails.

ⓘ **NOTE:** *PPDMHostName* is a mandatory option in the command line. If a value is not provided, but the agent service component has been installed by another agent, installation will succeed, but without PowerProtect, and hence it will not be possible to initiate backups from the UI. If, however, the agent service component has not been installed by another agent, then installation will fail. Specifying *ProductInstallPath* is optional, but if used, the value cannot be empty. When the *ProductInstallPath* value is provided during update or coexistence, but the install path is not the same as that of the previously installed file system or already installed agents, installation fails.

Windows installer logs are retained at `<System drive>\Users\<installing user>\AppData\Local\Temp`, and should be consulted in the event of an installation failure. In silent mode, any error message is logged only in the Windows installer logs.

Update the File System agent on Windows

If you are using an earlier version of PowerProtect Data Manager, the File System agent supports a direct update. You can update the PowerProtect Data Manager File System agent on supported Windows systems in interactive or silent mode.

Update and register the latest version of the PowerProtect Data Manager File System agent for Windows with the same PowerProtect Data Manager server in the same location.

ⓘ **NOTE:** When you install or update the File System agent, other application agents on the system must be updated to the same version as the File System agent.

Clustered environment requirements and considerations

The same version of the File System agent must be installed on each node in the cluster that is registered with PowerProtect Data Manager.

When the File System agent is updated from an earlier version, the following events occur:

1. Previous cluster assets with backup copies are displayed with a status of `Deleted` in **Infrastructure** > **Assets** > **File System**.
2. Previous cluster assets are removed from protection policies, but their backup copies can be restored. These backup copies are displayed under the name of the cluster node.
3. New cluster assets are discovered, and then displayed under the name of the logical cluster host in **Infrastructure** > **Assets** > **File System**.
4. New cluster assets with the same name as previous cluster assets are automatically added to the protection policies from which the previous cluster assets were removed.

Update the File System agent on Windows in interactive mode

Use this interactive procedure to update the File System agent on supported Windows systems.

Prerequisites

- Ensure that you carry out the prerequisites provided in File System agent prerequisites.
- Download the File System agent software package.

Steps

1. In the PowerProtect Data Manager UI:

   a. Click ⚙, and then select **Downloads** from the **System Settings** menu.

   b. Select the File System agent download package for Windows, `fsagent1912_win_x64.zip`.

   c. Download the package in the location that you want to install the File System agent.

      NOTE: During update, or fresh installation in case of coexistence, the File System agent will be installed on previous install path of the File System agent, or the path of a previously installed Application agent.

2. Run the `fsagent-19.12.0.0.exe` program.
3. Follow the update steps in the wizard to provide the installation location and the PowerProtect Data Manager server IP address.

   NOTE: If another application agent is already installed on the client and registered to PowerProtect, ensure that you register the agent with the existing PowerProtect Data Manager server IP. When you register the agent with a PowerProtect Data Manager server that is different from the currently registered server, no warning message appears, and requests are routed to the newer server instance.

   If PowerProtect Data Manager communications port 7000 is not enabled, you can change the firewall rule setting now as part of this update by selecting the **Configure the Windows Firewall** option under **Common Core Components**.

   NOTE:

   When the **Configure the Windows Firewall** option is enabled, the installation creates the Windows firewall rule that allows inbound and outbound connections for the agent service process. Installation of the File System agent requires port 7000 on the File System agent host and port 8443 on PowerProtect Data Manager to be open bidirectionally. These ports enable communication between the File System agent and PowerProtect Data Manager.

   If the Microsoft application agent is already installed and firewall rules are configured, then the **Configure the Windows Firewall** option is selected by default but disabled for the File System agent.

4. Click **Upgrade**.
   The following `msi` files are used for the installation:
   - `AgentService.msi`—Installs or updates the agent service component for File System agent.
   - `BBBWT.msi`—Installs the block-based backups driver.
   - `Fsagent.msi`—Installs the File System agent related files and folders.
5. Click **Finish**.

   NOTE: If a change occurred to the FQDN of the client, the installation completes successfully but the registration fails. To re-register the client to the correct FQDN, use the **Modify** option under **Add/Remove programs** for the File System agent, and then restart the agent service on the client.

Update the File System agent on Windows in silent mode

Use the following commands to perform a silent update of the File System agent on Windows.

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

```
fsagent-19.12.0.0.exe /s PPDMHostName=<PPDM_server_IP> ForceUpgrade=1
```

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

```
 fsagent-19.12.0.0.exe /s PPDMHostName=<PPDM_server_IP> ForceUpgrade=1
ProductInstallPath="D:\alternate_path"
```

To enable the PowerProtect Data Manager communications port 7000, if Windows firewall rules have not been previously configured, run:

```
fsagent-19.12.0.0.exe /s PPDMHostName=<PPDM_server_IP> EnableFirewallRules=1
ForceUpgrade=1
```

When `EnableFirewallRules` is enabled (set to '1'), the installation creates the Windows firewall rules that allow inbound and outbound connections for the agent service process. Installation of the File System agent requires port 7000 on the File System agent host and port 8443 on PowerProtect Data Manager to be open bidirectionally. These ports enable communication between the File System agent and PowerProtect Data Manager.

The change in EnableFirewallRules configuration will take place only on first-time installation or upgrade of the agent service.

> ⓘ **NOTE:** `PPDMHostName` is a mandatory option in the command line. If a value is not provided, but the agent service component has been installed by another agent, update will succeed, but without PowerProtect registration, so that it will not be possible to initiate backups from the UI. However, if the agent service component has not been installed by another agent, then update will fail. Specifying `ProductInstallPath` is optional, but if used, the value cannot be empty. When the `ProductInstallPath` value is provided during update or coexistence, but the install path is not the same as that of the previously installed file system or already installed agents, installation fails.

For File System agent silent update, or coexistence where common components are installed on the host:

- If common components are installed on the host, a File System agent update requires the additional option `ForceUpgrade=1`.
- All agents running on a client must be registered to the PowerProtect Data Manager server and must be updated to the same version.
- PowerProtect Data Manager does not support agents running different versions on the same client. Setting `ForceUpgrade=1` masks the prompt that requests users to update any other agents installed on that client to the same version to which the File System agent is being updated.

Uninstall the File System agent on Windows

On Windows, you can uninstall the File System agent with the setup file.

Steps

1. Launch `fsagent-19.12.0.0.exe`.
2. On the **Install Modification** page, select **Remove**, and then click **Next**.
3. On the **Configure Uninstallation Options** page, select **Yes** for each common component that you want to uninstall, and then click **Remove**.
4. On the **Complete the Setup** page, click **Finish**.

Results

The firewall rule created during installation for PowerProtect Data Manager communications port 7000 is removed automatically during the uninstall operation.

Silent uninstallation commands

Steps

1. To perform a silent uninstall without uninstalling common components (such as the PowerProtect agent service or BBB), run:

   ```
   fsagent-19.12.0.0.exe /s /uninstall
   ```

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

```
fsagent-19.12.0.0.exe /s /uninstall UnInstallPPDMAgent="1" UnInstallBBBWT="1"
```

> **NOTE:** If the File System agent is the last agent to be uninstalled, any common component that you do not uninstall remains on the host. You cannot uninstall the common components from the control panel.

Recommission the File System agent on Windows

You can use the procedure in this topic to onboard the decommissioned File System agent to the same PowerProtect Data Manager server.

> **NOTE:** You can use the **Modify** option under **Add/Remove programs** for the File System agent to recommission the File System agent with PowerProtect Data Manager only if you have not uninstalled the File System agent and PowerProtect agent service.
>
> If you have cleaned up the installation directories and manually uninstalled both the File System agent and PowerProtect agent service, then you must complete the installation procedures in Installing and updating the File System agent on Windows.

Alternatively, you can use the `register.bat` script to register and recommission the File System agent with PowerProtect Data Manager, as follows:

`<Install_folder>\AgentService\register.bat --enable`

Update the application agent in the PowerProtect Data Manager UI

Learn how to perform a precheck operation and update the application agent software on one or more hosts in the PowerProtect Data Manager UI.

Prerequisites

The precheck and update operations are only available for registered clients and application agent versions 19.10 and later.

> **NOTE:** On AIX, you cannot update the File System agent software in the PowerProtect Data Manager UI. You must use the `install.sh` script to update the File System agent on AIX from version 19.10 to 19.11.

Steps

To perform a precheck:

1. From the left navigation pane in the PowerProtect Data Manager UI, select **Infrastructure** > **Application Agents**.

   The **Application Agents** window opens.
2. Select the check box next to each application agent host to be included in the precheck.
   When the application agent versions on the selected hosts are 19.10 or later and the versions are earlier than the current PowerProtect Data Manager version, the **More Actions** button becomes enabled.
3. Click **More Actions** > **Precheck Update**.

   The **Precheck Update** window opens.
4. On the **Schedule Precheck** page:
   a. In the **Name** text box, type a name for the precheck operation.
   b. Select one of the following options:
      - **Precheck now**—Performs the precheck immediately.
      - **Precheck later**—Schedules the precheck to occur at a later time. If you select this option, specify the date and time to perform the precheck.

   c. Click **Next**.
5. On the **Summary** page, review the information for the selected application agent hosts, and then click **OK**.

The precheck verifies that the application agent hosts meet the minimum update requirements, including system memory, disk space, and version requirements. If the precheck passes, PowerProtect Data Manager downloads the update software package on each application agent host.

You can monitor the progress of the precheck operation in the **System Jobs** window.

To perform an update:

6. From the left navigation pane in the PowerProtect Data Manager UI, select **Infrastructure** > **Application Agents**.

   The **Application Agents** window opens.
7. Select the check box next to each application agent host to be included in the update.

   NOTE: In a cluster environment, select each host of the cluster; otherwise, any unselected hosts are automatically selected for the update. It is recommended that each host of a cluster has the same application agent version.

   When the application agent versions on the selected hosts are 19.10 or later and the versions are earlier than the current PowerProtect Data Manager version, the **More Actions** button becomes enabled.
8. Click **More Actions** > **Configure Update**.

   The **Configure Update** window opens.
9. On the **Schedule Updates** page:
   a. In the **Name** text box, type a name for the update operation.
   b. Select one of the following options:
      - **Update now**—Performs the update immediately.
      - **Update later**—Schedules the update to occur at a later time. If you select this option, specify the date and time to perform the update.
   c. Click **Next**.
10. On the **Summary** page, review the information for the selected application agent hosts, and then click **OK**.

    On each selected host, the update performs a precheck, places the host in maintenance mode, updates the application agent, and then returns the host to normal mode.

    You can monitor the progress of the update operation in the **System Jobs** window.

    When the update is complete, the update status of each host changes to **Up to date** in the **Application Agents** window.

    If the update fails:

    - An error is displayed, and you must manually return the hosts to normal mode.
    - Check the agent service logs for details on how to manually restore the host system.
    - Check the ADM logs for more information.
    - For detailed steps to downgrade to a previous version of the application agent, run the following command:

      ```
      ./pushupdate.sh -r -n
      ```

Manage the PowerProtect agent service

The PowerProtect agent service provides important functionality for the application agent operations with the PowerProtect Data Manager.

Review the following topics to ensure that you enable and manage the PowerProtect agent service functionality as required for application agent operations.

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 file system assets on PowerProtect Data Manager hosts, as well as their backup copies. After an initial discovery when the agent service discovers new assets and backup copies, the agent service notifies 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.
- 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. The PowerProtect Data Manager goes through the agent service to delete the catalog entries from the agent's local datastore.

  > **NOTE:** The manual deletion of backup copies is not recommended. PowerProtect Data Manager automatically deletes expired backup 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 AIX or 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
  ```

  Alternatively on Linux, you can use the following command to start the agent service:

  ```
  # service agentsvc start
  ```

- To stop the agent service:

  ```
  # register.sh --stop

  Successfully stopped agent-service.
  ```

  Alternatively on Linux, you can use the following command to stop the agent service:

  ```
  # service agentsvc stop
  ```

- 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.
  ```

- Alternatively on Linux, you can use the following command to obtain the status of the agent service when it is running or not running:

  ```
  # service agentsvc status
  ```

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 of 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.

3

Managing Storage, Assets, and Protection

Topics:

Manage the File System agent

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

About this task

> **NOTE:** PowerProtect Data Manager supports the coexistence of the following agents on the same host:
>
> - Microsoft SQL Server application agent and File System agent on Windows
> - Microsoft Exchange Server application agent and File System agent on Windows
> - Oracle RMAN agent and File System agent on AIX
> - Oracle RMAN agent and File System agent on Linux
> - SAP HANA agent and File System agent on Linux

Steps

1. Select **Infrastructure** > **Application Agents**.
2. In the **Application Agents** window, click **Add**.
3. Select one of the following options:
   - **Add FQDN**

     Perform the following steps:

     a. Type the fully qualified domain name (FQDN) for the application agent.
     b. Specify the date until which the application agent is pre-approved.
     c. Click **Save**.
   - **CSV Filename**

     Perform the following steps:

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

     > **NOTE:** The contents of the .CSV file must be in the following format, for example:
     >
     > ```
     > "ppdm.dell.com"
     > "ppdm2.emc.com"
     > "ppdm.dellemc.com"
     > ```

    The **Explorer** window appears.

   b. Select the `.csv` file, and then click **Open**.

      The file appears in the window.

   c. Select the date until which the application or File System agent is pre-approved.
   d. Click **Save**.

4. The `Auto Allow List` option is disabled by default. When `Auto Allow List` is enabled, all pre-approved Application Agents are automatically approved.

   If you leave the `Auto Allow List` option disabled, select an application agent, and then select one of the following options:

   - **Approve**
   - **Reject**
   - **Edit**, and then make the required changes.
   - **Remove**

View application agent details

Use the **Application Agents** window in the PowerProtect Data Manager UI to monitor the registration and update status of application agents, and view details for individual application agents.

To view application agent details, from the left navigation pane, select **Infrastructure** > **Application Agents**.

Agent registration status displays the total number of application agents that are awaiting approval, approved, registered, or rejected.

Agent update status displays the total number of application agents that are up-to-date, available, scheduled, in progress, or failed.

NOTE: If the update of an application agent fails for any reason, the agent host is counted as available. The host is included in the total number of available applicant agents.

At the end of the **Agent update status** row, you can click the arrow to view information about scheduled updates. The **Schedules** table appears and displays the following information:

- Update/Precheck Name
- Date and Time
- Schedule Status
- Host Count
- Actions

The lower table in the **Application Agents** window displays information about individual application agents. The following table describes the available information.

Table 7. Application agent information

Column	Description
Details	Click 🔍 in the **Details** column to view details and summary information for the application agent, including registration status.
Host Name	The name of the application agent host.
IP	The IPv4 or IPv6 address of the application agent host.
Registration Status	The registration status of the application agent: ● Awaiting Approval ● Pending Approval ● Registered ● Approved ● Rejected ● Expired ● Accepting Certificates ● Failed

Table 7. Application agent information (continued)

Column	Description
OS	The operating system of the application agent host.
Agent Type	The application agent type.
Current Version	The current version of the application agent.
Update Status	The update status of the application agent host: ● Available—The PowerProtect Data Manager release is 19.12 and the application agent release is 19.10 or 19.11. ● In Progress—The update of the application agent is in progress. ● Up to Date—The PowerProtect Data Manager release and the application agent release are both 19.12. ● Scheduled—The application agent is scheduled for an update. ● Failed—The update of the application agent failed. ● Not Supported—The PowerProtect Data Manager release is 19.12 and application agent release is earlier than 19.10.

Filter and sort information

Use the filtering and sorting options to find specific application agents, and to organize the information that you see.

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.

Use the **Search** field to filter application agents 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.

Export application agent data

To export the data that is shown in the table to a .CSV file, click **Export All**.

For more information about the **Export All** functionality, see the *PowerProtect Data Manager Administration and User Guide*.

Enable an asset source

An asset source 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.

In some circumstances, the enabling of multiple asset sources is required. For example, a vCenter Server and a Kubernetes cluster asset source must be enabled for Tanzu Kubernetes guest cluster protection.

There are other 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 though the API or the PowerProtect Data Manager user interface, 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 user interface. On a new deployment, however, no asset sources are enabled by default.

Steps

1. From the PowerProtect Data Manager user interface, 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 host, select **Infrastructure** > **Application Agents** and click **Add** or **Approve** as required.

ⓘ **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 Server virtual machines, then you cannot disable the vCenter Server asset source. But if you register a vCenter server and then delete it 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.

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 are removed automatically as part of daily PowerProtect Data Manager cleanup after all associated backup copies have been deleted. These assets can also be removed 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.

Discover a file system host

Perform the following steps to discover a file system host as an asset source in the PowerProtect Data Manager UI.

Steps

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

   The **Asset Sources** window appears.
2. Select the agent host tab.
3. Select the file system host and click **Discover**.

   The **Initiate Discovery** dialog appears with an option to immediately start a full discovery of the assets on the host.

   > **NOTE:** From the agent host tab, you can click **Discover** at any time if any additions or other changes to your asset sources have taken place outside of the PowerProtect Data Manager environment. Asset discovery is also initiated by default after registration of the host to PowerProtect Data Manager and at hourly intervals. Discovery time is based on networking bandwidth. Each time you initiate a discovery process, the resources that are discovered and those that are handling the discovery impact system performance.
4. Click **Yes**.

Results

When the File System asset source is configured correctly, you can add the file system assets to a PowerProtect Data Manager protection policy. Go to **Infrastructure** > **Assets**, and then select the **File Systems** tab. Use ⊞ ≡ to switch between a list view of all file system assets for all of the discovered File System hosts and a hierarchical view of assets within each File System host that has been discovered in PowerProtect Data Manager.

Adding a protection policy for File System protection

Use the PowerProtect Data Manager UI to add a protection policy to protect File System data.

Review the prerequisites in the section File System agent prerequisites.

Before you perform a backup on a weekly or monthly schedule from the protection policy, set the PowerProtect Data Manager time zone to the local time zone. If the PowerProtect Data Manager time zone is not set to the local time zone, the weekly or monthly backup still runs but triggers based on the PowerProtect Data Manager time zone.

The *PowerProtect Data Manager Administration and User Guide* provides more information about working with storage units, such as the relationships between storage units and policies, and applicable limitations.

If applicable, complete all of the virtual network configuration tasks before you assign any virtual networks to the protection policy. The *PowerProtect Data Manager Administration and User Guide* provides more information.

> **NOTE:** PowerProtect Data Manager does not support the automatic retention lock (ARL) setting on the DD system. The option to create a storage unit during protection policy configuration does not support compliance mode retention locking, only governance mode. To use compliance mode retention locking, create and configure a storage unit before you configure an associated protection policy. If you enable retention locking and select a storage unit where the retention lock mode is `None`, the retention lock defaults to governance mode. The *PowerProtect Data Manager Administration and User Guide* provides more information.

Policy types and purposes

Each File System protection policy has a type that defines the purpose of the policy. When you add a protection policy, select one of the available types:

- **Centralized Protection**—Use PowerProtect Data Manager to manage all aspects of protection.
- **Self-Service Protection**—Use the File System agent to create local backup protection. PowerProtect Data Manager creates a protection policy and manages extra objectives.
- **Exclusion**—Use this type if there are assets within the protection policy that you plan to exclude from data protection operations.

For clarity, this guide provides separate instructions for adding a protection policy of each type, even though some of the steps overlap. The terminology for each task differs slightly where the available objectives differ between policy types. Complete only the task that applies to your goal.

Replication triggers

PowerProtect Data Manager orchestrates protection policy replication objectives independently of the primary backup. When you add a replication objective to a policy, select one of the available triggers.

The default replication trigger is a schedule window that you define by setting a recurrence period plus start and end times. Replication occurs during the defined window. For example, every day between 8 p.m. and 12 a.m.

You can also trigger replication immediately after the completion of the associated primary backup, whether scheduled or manual. At the start of the primary backup, PowerProtect Data Manager generates an associated replication job that remains queued until the end of the protection job. If the backup fails or completes with exception, the associated replication job is skipped. Restarting the protection job queues the associated replication job again.

When you create a replication objective, you can specify either scheduled replication or replication after backup completion, which is applicable to both centralized and self-service protection policies.

> **NOTE:** For replication after backup completion, PowerProtect Data Manager 19.12 or later and application agents 19.10 or later are required. It is recommended that you update the application agents to the latest version.

Using a schedule can help you manage network traffic by replicating during off-peak hours. However, for larger backup sets, the primary backup may not finish before the start of the replication schedule, which creates a replication backlog. Replication after backup completion prevents a replication backlog from forming.

To prevent data loss, the replication after backup completion trigger replicates new backups from the primary objective and any outstanding backups that have not yet replicated.

Add a protection policy for centralized File System protection

With centralized protection, PowerProtect Data Manager manages all aspects of the protection process. The process of adding a protection policy is similar for all policy types. However, these instructions contain only elements and options that appear when you select the centralized protection policy type.

Prerequisites

Review the prerequisites in Adding a protection policy for File System protection.

Steps

1. Select **Protection** > **Protection Policies**.

   The **Protection Policy** window appears.
2. Click **Add**.

   The **Add Policy** window appears.
3. In the **Type** page, specify the new protection policies group fields. For example, if you are creating a protection policy for daily backups in the Windows server:
   a. In the **Name** field, specify the name of the protection policy. For example, `File System Prod`.
   b. In the **Description** field, specify a short description of the protection policy. For example, `File System Prod Daily Backups`

c. In the **Type** field, select **File System**.

d. Click **Next**.
The **Purpose** page appears.

4. To manage all protection centrally, click **Centralized Protection**.
5. Click **Next**.
The **Assets** page appears.
6. Select the unprotected assets that you want to add to the backup of this protection policy group. The window enables you to filter by asset name to locate the required assets.

   You can use to switch between a list view of all assets discovered by PowerProtect Data Manager and a hierarchical view to display the assets in a tree structure underneath each host. A hierarchical view can be helpful if you have added multiple file systems and need to more easily identify which assets belong to which host.
7. Click **Next**.
The **File Exclusions** page appears.
8. Optionally, to enable exclusions, click **Enable**.

   a. Select one or more filters to apply, provide the parameters, and click **Add Filter**.

      Click **Add a saved filter** to use an existing filter or group of filters as a template.

      NOTE: Add an exclusion filter provides more details about exclusion filters.

   b. Enter a name and description for the filter and click **Save**.

      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.

   The *PowerProtect Data Manager Administration and User Guide* 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 backup copies only the changed data since the last backup to create a new full backup.
    - **Retain For**—Specify the retention period for the synthetic full backup.
    - **Start** and **End**—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.

      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:

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

    - **Create a Full...**—Specify whether you want to create an hourly, daily, weekly, monthly, or yearly full backup.
    - **Repeat on**— Depending on the frequency of the full backup schedule, specify the hour of the day, day of the week, or the date of the month that the full backup occurs.
    - **Retain For**—

      CAUTION: The retention period of synthetic full backups must be less than or equal to the retention period of full backup copies. If you set a shorter retention period for a synthetic full backup than for the corresponding full backup, then data loss might occur and you might be unable to recover the point-in-time copies.

      By default, the retention period for the full backup is the same as that for the synthetic full backup. You can, however, specify a retention period for the full backup that is longer than the retention period for the synthetic full backup.
    - **Start** and **End**—The activity window. Specify a time of day to start the full backup, and a time of day after which 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.

c. Click **Add Backup** and repeat the procedure for creating full backups if you want to create additional backup copies at different intervals with different retention periods.

   Within this protection policy, when a full schedule conflicts with another full backup schedule, a message appears, indicating that there is a conflict. Schedule occurrences can conflict with each other when the activity windows are identical or occur entirely within the same time range. To avoid full schedule conflicts in a policy, edit the activity windows.

   If you proceed with conflicting schedules, the backup of the lower priority schedule will be skipped. Schedule priority is ranked according to the following criteria:

   - Full schedules have a higher priority than Synthetic Full schedules.
   - For schedules of the same backup type, the schedules that run less frequently have a higher priority than schedules that run more frequently.
   - For schedules with the same backup type and frequency, the schedule with the longest activity window has the higher priority. If the activity windows are also identical, only one of these schedules will run.

   ⓘ **NOTE:** When a schedule conflict between full backups occurs, PowerProtect Data Manager retains the full backup with the longest retention period.

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 protection storage 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 **New** if 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, `testvmpolicy-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 at policy completion. For example, `testvmpolicy-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.

      The retention lock mode setting comes from the configuration of the selected storage unit. When you enable retention locking, the **Retention Lock Mode** field displays the corresponding storage unit setting.

      Setting a retention lock 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** dialog to a minimum number of 14 days so that the replicated backup does not expire before the primary backup.

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

      The *PowerProtect Data Manager Administration and User Guide* 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**.

   After completing the objective, you can change any details by clicking **Edit** next to the objective.

14. Optionally, replicate the backups:

   ⓘ **NOTE:**

   To enable replication, ensure that you add remote protection storage as the replication location. The *PowerProtect Data Manager Administration and User Guide* provides detailed instructions about adding remote protection storage.

   When creating multiple replicas for the same protection policy, it is recommended to select a different storage system for each copy. If you select a storage unit that is the target of another objective for the same policy, the UI issues a warning. The *PowerProtect Data Manager Administration and User Guide* provides information about replicating to shared protection storage to support PowerProtect Cyber Recovery. Verify the storage targets and the use case before you continue.

   When you create a replication objective, you can specify either scheduled replication or replication after backup completion.

ⓘ **NOTE:** For replication after backup completion, PowerProtect Data Manager 19.12 or later and application agents 19.10 or later are required. It is recommended that you update the application agents to the latest version.

a. Click **Replicate** next to **Primary Backup**. An entry for **Replicate** is created to the right of the primary backup objective.
b. Under **Replicate**, click **Add**.
The **Add Replication** dialog appears, with information in the left pane for each schedule that has been added for the primary backup objective of this protection policy.

ⓘ **NOTE:** Backups for all of the listed schedules will be replicated. You cannot select individual schedules for replication.

c. Select a storage target:

- **Storage Name**—Select a destination from the list of protection storage. Or, select **Add** to add a protection storage system and complete the details in the **Storage Target** window.
- **Storage Unit**—Select an existing storage unit on the protection storage system. Or, select **New** to automatically create a storage unit.
- **Network Interface**—Select a network interface from the list, if applicable.
- **Retention Lock**—Move the **Retention Lock** slider to the right to enable retention locking for these replicas.

  The retention lock mode setting comes from the configuration of the selected storage unit. When you enable retention locking, the **Retention Lock Mode** field displays the corresponding storage unit setting.
- **SLA**—Select an existing replication service level agreement that you want to apply to this schedule from the list. Or, select **Add** to create a replication SLA within the **Add Service Level Agreement** wizard.

The *PowerProtect Data Manager Administration and User Guide* provides more information about replication targets, such as SLAs.

d. Select when to replicate the backups:

Replication triggers provides more information.

- To replicate after the backup finishes, move the **Replicate immediately upon backup completion** slider to on.
- For scheduled replication, move the **Replicate immediately upon backup completion** slider to off, and then complete the schedule details in the **Add Replication** dialog.

  For replication of the primary backup, the schedule frequency can be every day, week, month, or *x* hours.

  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 from 1 to 12 hours.

By default, all replicas of the primary backup objective inherit the retention period from the **Retain For** value of the synthetic full and full backup schedules.

e. To specify a different retention period for individual synthetic full and full replicas, clear **Set the same retention time for all replicated copies**, click **Edit** in the row of each schedule that you want to change, update the value in the **Retain For** field, and then click **Save**.

⚠ **CAUTION: Setting a retention period for the replicas of other backup types (such as log backups, incremental, and differential backups, where applicable) that is shorter than the retention period of the corresponding full backup may result in being unable to recover from those replicas.**

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

15. Optionally, to move backups from protection storage to Cloud Tier, add a Cloud objective for the primary or replication objective:

ⓘ **NOTE:** To move a backup or replica to Cloud Tier, objectives must have a retention time of 14 days or more. PowerProtect Data Manager also requires the discovery of protection storage with a configured Cloud unit.

a. Click **Cloud Tier** next to **Primary Backup**. Or, if adding a Cloud objective for a replication objective that you have added, click **Cloud Tier** under **Replicate**.
An entry for **Cloud Tier** is created to the right of the primary backup objective, or below the replication objective.
b. Under the entry for **Cloud Tier**, click **Add**.
The **Add Cloud Tier Backup** dialog appears, with summary information for the parent objective to indicate whether you are adding this Cloud Tier objective for the primary backup objective or the replication objective.

c. Keep the **All applicable full backups** slider to the right if you want to tier the backups from all of the full primary backup or replication schedules of this policy. Otherwise, move the slider to the left and select the full schedule(s) that you want to tier.

> ⓘ **NOTE:** If the retention period of a schedule is less than the minimum 14 days required before tiering occurs, or is less than the value in the **Tier After** field, you can still select this schedule for tiering. However, if you do not edit the retention period of this schedule or its backup or replication copy to a value greater than the **Tier After** field before the retention period of the copy expires, the backup or replication copy of this schedule will not be cloud tiered.

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

The *PowerProtect Data Manager Administration and User Guide* provides detailed instructions for adding a Cloud objective for a primary or replication objective.

16. Click **Next**.
The **Options** page appears.
17. On the **Options** page, select the additional option if required for the policy:

- **Enable indexing for file search and restore** — Select this to perform search on the backups.
- **Troubleshooting** — Select this option to enable the debug logs for troubleshooting at higher debug levels. To override the default debug level, add the statement `debugLevel=<N>` to the `addOn.cfg` configuration file, where `N` is the desired debug level, in the range [4..9].

> ⓘ **NOTE:** Overriding the bug level in this manner may result in larger logs that may slow backup operations.

In Windows environments, the impacted logs include:

- `FSAgentInstallPath\logs\vsscr.log`
- `FSAgentInstallPath\logs\nsriscsi.log`
- `FSAgentInstallPath\logs\nsriscsi_***.log`
- `FSAgentInstallPath\logs\nsrwriter.log`
- `FSAgentInstallPath\logs\ddfscon.***.log`
- `FSAgentInstallPath\logs\ddfscon_***.log`
- `FSAgentInstallPath\logs\ddfssv.log`
- `FSAgentInstallPath\logs\ddfssv_***.log`
- `FSAgentInstallPath\logs\ddfsrc_***.log`

In Linux environments, the impacted logs include:

- `/opt/dpsapps/fsagent/logs/nsriscsi.log`
- `/opt/dpsapps/fsagent/logs/ddfscon.***.log`
- `/opt/dpsapps/fsagent/logs/ddfssv.log`

> ⓘ **NOTE:** If you have updated from an earlier File System agent version, some log files may appear with both `.log` and `.raw` extensions. Use the `.log` files.

18. Click **Next**.
The **Summary** page appears.
19. Review the protection policy group configuration details. You can click **Edit** next to any completed window's details to change any information. When completed, click **Finish**.
An informational message appears to confirm that PowerProtect Data Manager has saved the protection policy.

When the new protection policy is created and assets are added to the protection policy, PowerProtect Data Manager performs backups according to the backup schedule.
20. 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.
Upon requesting a backup (file-based or block-based), the status of the protection policy becomes **Queued**. This status switches to **Running** only after the system begins writing the backup to protection storage.

Add a protection policy for self-service File System protection

With self-service protection, the agent or host controls the primary backup process and PowerProtect Data Manager manages other aspects of the protection process. The process of adding a protection policy is similar for all policy types. However, these instructions contain only elements and options that appear when you select the self-service protection policy type.

Prerequisites

Review the prerequisites in Adding a protection policy for File System protection.

Steps

1. Select **Protection** > **Protection Policies**.

   The **Protection Policy** window appears.

2. Click **Add**.

   The **Add Policy** window appears.

3. In the **Type** page, specify the new protection policies group fields. For example, if you are creating a protection policy for daily backups in the Windows server:

   a. In the **Name** field, specify the name of the protection policy. For example, **`File System Prod`**.

   b. In the **Description** field, specify a short description of the protection policy. For example, **`File System Prod Daily Backups`**

   c. In the **Type** field, select **File System**.

   d. Click **Next**.
      The **Purpose** page appears.

4. To create local backup protection, click **Self-Service Protection**.

5. Click **Next**.
   The **Assets** page appears.

6. Select the unprotected assets that you want to add to the backup of this protection policy group. The window enables you to filter by asset name to locate the required assets.

   You can use to switch between a list view of all assets discovered by PowerProtect Data Manager and a hierarchical view to display the assets in a tree structure underneath each host. A hierarchical view can be helpful if you have added multiple file systems and need to more easily identify which assets belong to which host.

7. 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.

   The *PowerProtect Data Manager Administration and User Guide* provides instructions.

8. Click **Add** under **Primary Retention**.
   The **Add Primary Retention** dialog appears.

9. In the **Retentions (Self Service)** pane, specify the retention period.

   By default, all backup types have the same retention period. Changing the retention periods for specific backup types requires File System agent 19.9 or later. To change the retention periods for specific backup types, clear **Set the same retention time for all backup types** and change the **Retain *<backup_type>* For** field values as required.

   When a different retention time for all backup types is set, you can create additional full backup patterns with different retention times. For example, you can add a full backup pattern **`Retain full backups created every week on the Monday and Tuesday for 2 months`**.

   Self-service retentions created with older versions of the File System agent continue to use the same retention period for full and synthetic full backups.

10. On the **Target** pane of the **Add Primary Retention** 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 protection storage 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 **New** if 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, **`testvmpolicy-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 at policy completion. For example, **`testvmpolicy-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.

    The retention lock mode setting comes from the configuration of the selected storage unit. When you enable retention locking, the **Retention Lock Mode** field displays the corresponding storage unit setting.

Setting a retention lock 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** dialog to a minimum number of 14 days so that the replicated backup does not expire before the primary backup.

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

The *PowerProtect Data Manager Administration and User Guide* provides instructions.

11. 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 protection storage system under **Primary Retention**.

After completing the objective, you can change any details by clicking **Edit** next to the objective.

12. Optionally, replicate the backups:

> **NOTE:**
>
> To enable replication, ensure that you add remote protection storage as the replication location. The *PowerProtect Data Manager Administration and User Guide* provides detailed instructions about adding remote protection storage.
>
> When creating multiple replicas for the same protection policy, it is recommended to select a different storage system for each copy. If you select a storage unit that is the target of another objective for the same policy, the UI issues a warning. The *PowerProtect Data Manager Administration and User Guide* provides information about replicating to shared protection storage to support PowerProtect Cyber Recovery. Verify the storage targets and the use case before you continue.

When you create a replication objective, you can specify either scheduled replication or replication after backup completion.

> **NOTE:** For replication after backup completion, PowerProtect Data Manager 19.12 or later and application agents 19.10 or later are required. It is recommended that you update the application agents to the latest version.

a. Click **Replicate** next to **Primary Retention**. An entry for **Replicate** is created to the right of the primary objective.

b. Under **Replicate**, click **Add**.
The **Add Replication** dialog appears, with information in the left pane for each schedule that has been added for the primary backup objective of this protection policy.

> **NOTE:** Backups for all of the listed schedules will be replicated. You cannot select individual schedules for replication.

c. Select a storage target:

- **Storage Name**—Select a destination from the list of protection storage. Or, select **Add** to add a protection storage system and complete the details in the **Storage Target** window.
- **Storage Unit**—Select an existing storage unit on the protection storage system. Or, select **New** to automatically create a storage unit.
- **Network Interface**—Select a network interface from the list, if applicable.
- **Retention Lock**—Move the **Retention Lock** slider to the right to enable retention locking for these replicas.

  The retention lock mode setting comes from the configuration of the selected storage unit. When you enable retention locking, the **Retention Lock Mode** field displays the corresponding storage unit setting.
- **SLA**—Select an existing replication service level agreement that you want to apply to this schedule from the list. Or, select **Add** to create a replication SLA within the **Add Service Level Agreement** wizard.

The *PowerProtect Data Manager Administration and User Guide* provides more information about replication targets, such as SLAs.

d. Select when to replicate the backups:

Replication triggers provides more information.

- To replicate after the backup finishes, move the **Replicate immediately upon backup completion** slider to on.
- For scheduled replication, move the **Replicate immediately upon backup completion** slider to off, and then complete the schedule details in the **Add Replication** dialog.

For replication of the primary backup, the schedule frequency can be every day, week, month, or *x* hours.

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 from 1 to 12 hours.

By default, all replicas of the primary backup objective inherit the retention period from the **Retain For** value of the synthetic full and full backup schedules.

e. To specify a different retention period for individual synthetic full and full replicas, clear **Set the same retention time for all replicated copies**, click **Edit** in the row of each schedule that you want to change, update the value in the **Retain For** field, and then click **Save**.

   ⚠ **CAUTION: Setting a retention period for the replicas of other backup types (such as log backups, incremental, and differential backups, where applicable) that is shorter than the retention period of the corresponding full backup may result in being unable to recover from those replicas.**

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

13. Optionally, to move backups from protection storage to Cloud Tier, add a Cloud objective for the primary or replication objective:

    ⓘ **NOTE:** To move a backup or replica to Cloud Tier, objectives must have a retention time of 14 days or more. PowerProtect Data Manager also requires the discovery of protection storage with a configured Cloud unit.

    a. Click **Cloud Tier** next to **Primary Retention**. Or, if adding a Cloud objective for a replication objective that you have added, click **Cloud Tier** under **Replicate**.
    An entry for **Cloud Tier** is created to the right of the primary objective, or below the replication objective.
    b. Under the entry for **Cloud Tier**, click **Add**.
    The **Add Cloud Tier Backup** dialog appears, with summary information for the parent objective to indicate whether you are adding this Cloud Tier objective for the primary objective or the replication objective.
    c. Keep the **All applicable full backups** slider to the right if you want to tier the backups from all of the full primary backup or replication schedules of this policy. Otherwise, move the slider to the left and select the full schedule(s) that you want to tier.

       ⓘ **NOTE:** If the retention period of a schedule is less than the minimum 14 days required before tiering occurs, or is less than the value in the **Tier After** field, you can still select this schedule for tiering. However, if you do not edit the retention period of this schedule or its backup or replication copy to a value greater than the **Tier After** field before the retention period of the copy expires, the backup or replication copy of this schedule will not be cloud tiered.

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

       The *PowerProtect Data Manager Administration and User Guide* provides detailed instructions for adding a Cloud objective for a primary or replication objective.

14. Click **Next**.
    The **Options** page appears.
15. On the **Options** page, select the additional option if required for the policy:
    - **Enable indexing for file search and restore** — Select this to perform search on the backups.
    - **Troubleshooting** — Select this option to enable the debug logs for troubleshooting at higher debug levels. To override the default debug level, add the statement `debugLevel=<N>` to the `addOn.cfg` configuration file, where `N` is the desired debug level, in the range [4..9].

      ⓘ **NOTE:** Overriding the bug level in this manner may result in larger logs that may slow backup operations.

      In Windows environments, the impacted logs include:

      - `FSAgentInstallPath\logs\vsscr.log`
      - `FSAgentInstallPath\logs\nsriscsi.log`
      - `FSAgentInstallPath\logs\nsriscsi_***.log`
      - `FSAgentInstallPath\logs\nsrwriter.log`
      - `FSAgentInstallPath\logs\ddfscon.***.log`
      - `FSAgentInstallPath\logs\ddfscon_***.log`
      - `FSAgentInstallPath\logs\ddfssv.log`
      - `FSAgentInstallPath\logs\ddfssv_***.log`
      - `FSAgentInstallPath\logs\ddfsrc_***.log`

In Linux environments, the impacted logs include:

- `/opt/dpsapps/fsagent/logs/nsriscsi.log`
- `/opt/dpsapps/fsagent/logs/ddfscon.***.log`
- `/opt/dpsapps/fsagent/logs/ddfssv.log`

> **NOTE:** If you have updated from an earlier File System agent version, some log files may appear with both `.log` and `.raw` extensions. Use the `.log` files.

16. Click **Next**.
    The **Summary** page appears.
17. Review the protection policy group configuration details. You can click **Edit** next to any completed window's details to change any information. When completed, click **Finish**.
    An informational message appears to confirm that PowerProtect Data Manager has saved the protection policy.

    When the new protection policy is created and assets are added to the protection policy, PowerProtect Data Manager performs backups according to the backup schedule.
18. Click **OK** to exit the window, or click **Go to Jobs** to open the **Jobs** window to monitor the backup of the new protection policy group.

    You can monitor and view detailed information in the **Jobs** window for self-service backups and restores of database application agents.

    > **NOTE:**
    >
    > The **Cancel** and **Retry** options are not available for self-service jobs that are created by database application agents.
    >
    > When a backup fails or a backup is skipped, the backup job steps appear as canceled for the particular database. The backup job steps are displayed on the **Step Log** tab in the details section of the **Job ID Summary** window.

    Upon requesting a backup (file-based or block-based), the status of the protection policy becomes **Queued**. This status switches to **Running** only after the system begins writing the backup to PowerProtect DD.

Add a policy to exclude assets from data protection operations

An exclusion policy prevents the File System agent from including certain assets in a protection policy, for example, assets that you intend to back up separately. The process of adding a policy is similar for all policy types. However, these instructions contain only elements and options that appear when you select the exclusion policy type.

Prerequisites

Review the prerequisites in Adding a protection policy for File System protection.

Steps

1. Select **Protection** > **Protection Policies**.

   The **Protection Policy** window appears.
2. Click **Add**.

   The **Add Policy** window appears.
3. In the **Type** page, specify the new protection policies group fields. For example, if you are creating a protection policy for daily backups in the Windows server:
   a. In the **Name** field, specify the name of the protection policy. For example, **`File System Prod`**.
   b. In the **Description** field, specify a short description of the protection policy. For example, **`File System Prod Daily Backups`**
   c. In the **Type** field, select **File System**.
   d. Click **Next**.
      The **Purpose** page appears.
4. To exclude assets within the protection policy from data protection operations, click **Exclusion**.
5. Click **Next**.
   The **Assets** page appears.
6. Select the unprotected assets that you want to add to the backup of this protection policy group. The window enables you to filter by asset name to locate the required assets.

You can use to switch between a list view of all assets discovered by PowerProtect Data Manager and a hierarchical view to display the assets in a tree structure underneath each host. A hierarchical view can be helpful if you have added multiple file systems and need to more easily identify which assets belong to which host.

7. Click **Next**.
   The **Summary** page appears.
8. Review the protection policy group configuration details. You can click **Edit** next to any completed window's details to change any information. When completed, click **Finish**.
   An informational message appears to confirm that PowerProtect Data Manager has saved the protection policy.

   When the new protection policy is created and assets are added to the protection policy, PowerProtect Data Manager performs backups according to the backup schedule.
9. 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.

Cancel a File System agent backup or restore job

You can cancel a File System agent protection job (backup or restore) from the PowerProtect Data Manager UI. The job must be in a queued or running state. The backup or restore job runs for a primary backup that is configured through a File System agent protection policy.

About this task

You can perform two types of application agent job cancellations in the PowerProtect Data Manager UI:

- Cancellation of a job group that includes one or more asset jobs.
- Cancellation of an individual asset job.

> **NOTE:**
> - On a Linux platform, if a block-based image restore fails, or if you cancel a block-based image restore while it is Running, you must manually mount the target volume before next attempting any backup or restore on the same volume.
> - Upon cancellation of an incremental block-based backup, the next backup is promoted automatically to a full backup.
> - When a job completes before the cancel request reaches the application host, the status of the canceled job transitions to either success or failure.
> - You can cancel many other types of jobs, in addition to protection jobs. The *PowerProtect Data Manager Administration and User Guide* provides more information.

Perform the following steps to cancel an application agent protection job in the PowerProtect Data Manager UI.

Steps

1. 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.

2. In the **Protection Jobs** window, perform the required type of job cancellation:
   - To cancel a job group:
     a. In the **Protection Jobs** window, select the required job group and click **Cancel**.

        A job group warning prompt appears.

     b. Click **OK** at the prompt.

     You can monitor the job group cancellation in the **Protection Jobs** window. The job group status changes to Canceled when the cancellation of all the asset jobs is complete.

     To monitor the cancellation of individual asset jobs within the job group, click the job ID in the **Protection Jobs** window. The **Job ID Summary** window opens, where you can view the status of each asset job.

   - To cancel an asset job:
     a. In the **Protection Jobs** window, click the job ID.

        The **Job ID Summary** window opens to display the job details of the assets in the job group.

     b. In the **Job ID Summary** window, select the required asset job and click **Cancel**.

A job warning prompt appears.

c. Click **OK** at the prompt.

You can monitor the asset job cancellation in the **Job ID Summary** window. The asset job status changes to Canceled when the job cancellation is complete.

ⓘ **NOTE:** When the cancel request for a job cannot be completed, an informational alert is displayed.

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. Also, the **Extended Retention** SLA applies to protection policies created in PowerProtect Data Manager 19.11 and earlier only. The Extended Retention objective was removed in PowerProtect Data Manager 19.12. When updating to PowerProtect Data Manager 19.12 from a previous release, any protection policies created in the earlier release with the **Extended Retention** SLA will continue to be supported, however, you will not be able to edit the **Extended Retention** SLA in these policies.

In the **SLA Compliance** window, you can export compliance data by using the **Export All** functionality.

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.
   - **Replication**. If you choose this type, go to step 6.
   - **Cloud Tier**. If you choose this type, go to step 7.

   You can select only one type of Service Level Agreement.
4. If you selected **Policy**, specify the following fields regarding the purpose of the new Policy SLA:

   a. The **SLA Name**.

   b. If applicable, select **Minimum Copies**, and specify the number of Backup, 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 **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.

7. 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**.

8. 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**.

9. In the **Objectives** row of the **Summary** window, click **Edit**.

10. 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.
11. Click **Finish**.

    An informational message appears to confirm that PowerProtect Data Manager has saved the protection policy.
12. Click **Go to Jobs** to open the **Jobs** window to monitor the backup and compliance results, or click **OK** to exit.

    > **NOTE:** Compliance checks occur automatically every day at 2 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.
13. In the **Jobs** window, click 🔍 next to an entry to view details on the SLA Compliance result.

Extended retention (for protection policies created in PowerProtect Data Manager 19.11 and earlier)

> **NOTE:** This section applies to protection policies created in PowerProtect Data Manager 19.11 and earlier only. For protection policies created in PowerProtect Data Manager 19.12, instead of using the **Extend Retention** objective to extend the retention period of certain full copies, you can now add multiple full schedules for primary backup and replication objectives. When updating to PowerProtect Data Manager 19.12 from a previous release, any protection policies created in the earlier release with the **Extend Retention** objective will continue to be supported, however, you will not be able to edit existing extended retention objectives, or add new extended retention objectives, in these policies. The Knowledge Base article 000204454 at https://www.dell.com/support/ provides detailed information about specific **Extend Retention** objective migration scenarios when updating to PowerProtect Data Manager 19.12.

For protection policies created in PowerProtect Data Manager 19.11 and earlier, the **Extend Retention** objective allows you to 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 objective 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 a manual 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 objective 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 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 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 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 objective. 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 objective 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.

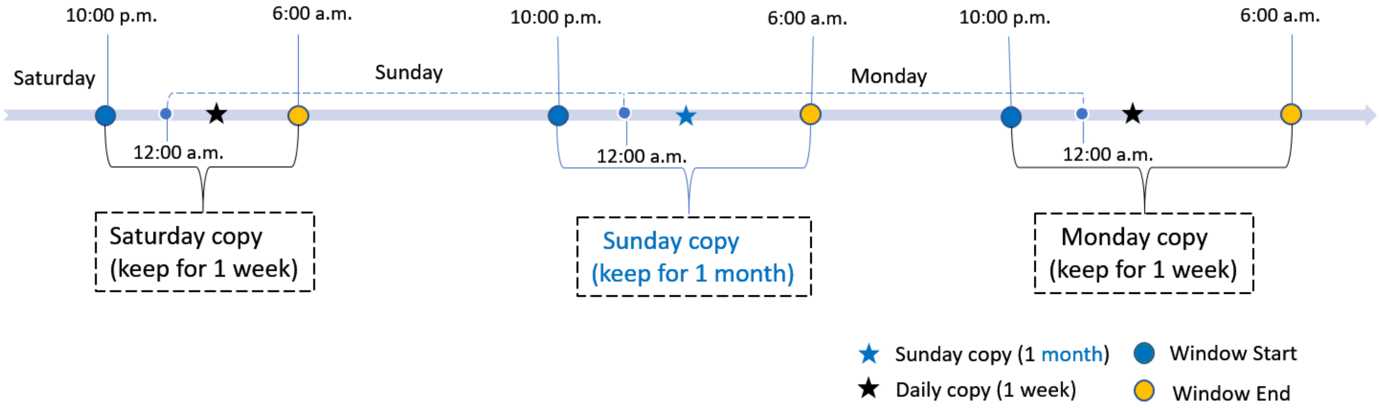

Figure 1. Extend retention backup behavior

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 objective 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.

Replication of extended retention backups

You can change the retention time of selected full primary backups in a replication objective by adding a replication objective to the extended retention backup. The rules in the extended retention objective define the selected full primary backups. Review the following information about replication of extended retention backups.

- Before you configure replication of extended retention backups, create a replication objective for the primary backup.
- Configure the replication objective of the extended retention and match this objective with one of the existing replication objectives based on the primary backup. Any changes to a new or existing storage unit in the extended retention replication objective or the replication objective of the primary backup is applied to both replication objectives.
- The replication objective of extended retention backups only updates the retention time of replicated backup copies and does not create any new backup copies in the replication storage.

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 the retention period for all asset types and backup types.

Steps

1. Select **Infrastructure** > **Assets**.
2. From the **Assets** window, select the tab for the asset type for which you want to edit the retention period. 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 from the table, and click **Edit Retention**.
6. Select 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 can 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 periods, and indicates whether the retention period has been extended or shortened.

Delete backup copies

In addition to deleting backups after the retention period expires, 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.
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 check box next to **Include latest copies**.
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**.

   ⓘ **NOTE:** If the data deletion is successful but the catalog deletion is unsuccessful, then the overall deletion job status appears as `Completed with Exceptions`.

   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 are 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 are 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 that 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.

      ⓘ **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** status from the table, and then click **Remove from PowerProtect**.
   The system displays a warning to confirm that 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.

Exclusion filters

Exclusion filters enable you to exclude certain files and folders from protection, based on the filter's conditions (conditions for exclusion).

Use the PowerProtect Data Manager UI to add, edit, and delete exclusion filters for file system files and folders.

When you create or edit a protection policy, you can apply exclusion filters to the protection policy.

When an exclusion filter is applied to a protection policy, the File System agent performs file-based backups of the protected assets. File-based backups traverse through the entire directory structure of the file system to back up all the files in each directory of the file system. While file-based backups can provide additional capabilities such as exclusion, these backups take longer to complete when compared to block-based backups.

ⓘ **NOTE:** Exclusion filters cannot be applied to self-service protection policies or to backups taken through self-service CLI.

Add an exclusion filter

Use the PowerProtect Data Manager UI to add filters that exclude specific files and folders based on certain conditions, such as file type, file size, modification time, and file path. When a file or folder meets the conditions, the filter excludes the data from the backup for the protection policy.

About this task

Use this procedure to add up to four filters for a file.

Steps

1. Select **Protection** > **File Exclusion**.
   The **File Exclusion** window appears.

2. Click **ADD**.
   The **Filter Information** window appears.
3. In the **Filter Name** field, type a name for the filter.
4. In the **Description** field, describe the purpose of the filter.
5. Select a filtering condition. You can add multiple filters.

   The filter excludes all files and folders that match these criteria from the backup for the protection policy. When you add multiple conditions, a file is excluded only if it meets all filter conditions. Within a filter, you can add a condition only once.

   Available filtering conditions:

   File Size Exclude files and folders that are larger or smaller than a specified size. Specify a value in either the **Greater than** or **Less than** field.

   File type Exclude files or folders based on file type. Specify a file name extension or multiple file name extensions that are separated by commas.

   Modified time Exclude files or folders that were modified before or after a certain date. Specify a date in either the **After** or **Before** field.

   Folder Path Exclude files and folders in a specific path. Specify the file path, and then enclose the file path in quotations. You can specify an absolute or relative path.

6. When you are finished building the filter, click **Add Filters**.
   The new filter appears in the table.
7. You can add up to four filters using the previous steps. When you are finished, click **Next**.
8. In the **Summary confirmation** page, verify the filter information and click **Finish**.

Guidelines for exclusion filters

Review the following guidelines for exclusion filters.

Using wildcards

Supported wildcards include an asterisk (`*`) to represent zero or more characters and a question mark (`?`) to represent zero or one character.

NOTE: Be careful when using the wildcard `*`. Depending on the wildcard location, you can match folders whose name matches the filter pattern and their contents, even when the names of those files do not match the filter. For example, `*\\log*.txt` also excludes files with the `.txt` extension in a folder whose name starts with `log`, even if the names of the files do not start with `log`.

Excluding by file type

The **File Type** filter enables you to exclude files and folders based on file extension.

You can specify a single extension or multiple file extensions. Separate multiple entries with a comma and do not add a space between entries. You can also specify related extensions by using wildcards. For example, `*.doc?` matches both `.doc` files and `.docx` files.

Excluding by type and path

You can combine extension and path to exclude all files of a particular type without respect to the file location.

For example `*\\log*.txt` matches all text files (`.txt`) where the file name starts with `log`, at any path.

You can also exclude all files of a particular type from a specific path. For example, `C:\\abc\\*.txt` matches all text files in the folder `C:\abc`. All matching files under subfolders of that specific path are recursively excluded.

You can combine these guidelines to exclude all files that match a specific name pattern under a particular path. For example, `C:\\folder\\log*.txt`.

Excluding by file path

The **Path** filter enables you to exclude files and folders in a specific path.

You can specify an absolute or relative path.

The following table provides examples for excluding files and folders using absolute and relative paths.

Table 8. Absolute and relative path examples

Type of path	Folder	File
Absolute	`F:\\folder1\\folder2\\*` In this example, the filter excludes all files and folders under `F:\folder1\folder2`.	`F:\\folder1\\folder2\\sample.txt` In this example, the filter excludes the `sample.txt` file under `F:\folder1\folder2`.

Relative	`*\\folder1\\folder2\\*`
	In this example, the filter excludes all files and folders under any volume with the hierarchy `folder1\folder2`.
	`D:\\*\\folder1\folder2\\*`
	In this example, the filter excludes all files and folders under any folder in `D:` with the hierarchy `folder1\folder2`.
		`*\\folder1\\folder2\\sample.log`
		In this example, the filter excludes all `sample.log` files under any volume with the hierarchy `folder1\folder2`.
		`D:\\*\\folder1\folder2\\sample.log`
		In this example, the filter excludes all `sample.log` files under any folder in `D:` with the hierarchy `folder1\folder2`.

Edit or delete an exclusion filter

Use the PowerProtect Data Manager to edit or delete an exclusion filter. You can change the filter name, description, logical operator, and filtering conditions.

Steps

1. Select **Protection** > **Filters**.

   The **Exclusion Filters** window appears, which displays the following information:
   - Name
   - Description
   - Conditions
   - Logical Operator
2. To edit a filter, complete the following tasks:
   a. Select a filter, and click **Edit**.
      The **Edit Exclusion Filter** wizard appears.
   b. Modify the desired fields, and then click **Next**.
      The **Summary** page appears.
   c. Click **Finish** to save your changes.
3. To delete a filter, select the filter that you want to delete, and then click **Delete**.

Apply an exclusion filter to a protection policy

When adding or editing a protection policy, you can apply a predefined exclusion filter to the protection policy. The **File Exclusions** page of the **Add Policy** or **Edit Policy** wizard enables you to select an exclusion filter and apply it to a protection policy.

Prerequisites

An exclusion filter must already exist.

About this task

To create a protection policy for file system protection and apply an exclusion filter to it, follow the steps in Add a policy to exclude assets from data protection operations.

To apply an exclusion filter to an existing protection policy, complete the following steps:

Steps

1. Select **Protection** > **Protection Policies**.

   The **Protection Policy** window appears.
2. Select a protection policy from the list, and then click **Edit**.

   The **Summary** page appears.
3. Click **File Exclusions** > **Edit**.
   The **File Exculsions** page appears.
4. Toggle the Disabled switch to enable exclusion.
5. Add a saved filter or build a new filter according to the steps provided in Add an exclusion filter.
6. Click **Next** twice, review the details on the **Summary** page, and click **Finish**.
   PowerProtect Data Manager applies the exclusion filter to the protection policy.

Results

After the backup starts, you can view details about the files that are excluded from the protection policy. To view the excluded files:
1. Open the **Jobs** window and select the job.
2. Click the **Details** icon to the left of the job name.
3. In the **Task Summary** section, click the link that indicates the total number of tasks.
4. Click the **Details** icon to the left of the task, and then review the protection policy details and excluded files.

Remove an exclusion filter from a protection policy

The **File Exclusions** page of the **Edit Policy** wizard enables you to remove an exclusion filter from a protection policy.

Steps

1. Select **Protection** > **Protection Policies**.

   The **Protection Policy** window appears.
2. Select a protection policy from the list, and then click **Edit**.

   The **Summary** page appears.
3. Select **File Exclusions** > **Edit**.
4. Clear the check box next to the filter that you want to remove from the protection policy.
5. Click **Next**.

   The **Summary** page appears.
6. Review the details, and click **Finish**.

Centralized restore of a file system asset

When file systems are protected within a protection policy in PowerProtect Data Manager, you can recover the file system data using the centralized image-level or file-level restore functionality in the PowerProtect Data Manager UI.

Prerequisites for restore of file system assets

Review the following requirements before performing centralized image-level or file-level restores of file system assets:

- Both the PowerProtect Data Manager server and client must be at a minimum version of PowerProtect Data Manager 19.3.
- Ensure that the File System agent is not installed and running on the target volume.

- Ensure that there is sufficient space on the target volume for the restore.
- Ensure that the target or destination volume is not read-only.
- Cross-platform support for centralized file-level restore is not supported. For example, you cannot recover a Windows backup on a Linux platform and the opposite way.
- Review the section Supported platform and OS versions for file system file-level restore.

Caution regarding image-level restore of a system volume to a system volume

Running an image-level restore from the backup of a system volume to a target volume that is the same or different system volume can cause the following problems:

- Files in use are not restored.
- The file system host machine may become unstable.

Therefore, in such a situation, it is recommended to perform a file-level restore for the required files and folders only.

Increasing the restore timeout

By default, the mount operation times out after 30 minutes and the backup copy is unmounted. When running file-level restores of large files, you can increase the restore timeout. Perform this task if file-level restores for large files timeout before completing.

1. Create a file with the name `browsersvc.cmd` in one of the following locations:
   - On Windows, `C:\Program Files\DPSAPPS\fsagent\settings`
   - On Linux, `/opt/dpsapps/fsagent/settings`
2. Add the following line to the file, and specify the same timeout value, in minutes, for both variables:

   ```
   {"-idletimeout":"timeout", "-resexpiry":"timeout"}
   ```

   For example, enter this line to set the restore timeout to 60 minutes:

   ```
   {"-idletimeout":"60", "-resexpiry":"60"}
   ```

Centralized image-level restore of a file system asset

A file system host image-level restore enables you to recover data from backups of file systems performed in the PowerProtect Data Manager UI.

Prerequisites

- On Linux, before performing an image-level restore of the block-based backup copy, ensure that you are not logged in to the destination file system asset (volume) for other data protection operations. If you are logged in to the destination asset (volume) for any other data protection operation, the restore fails.

Steps

1. From the PowerProtect Data Manager UI, select **Restore** > **Assets**, and then select the **File System** tab.

   The **Restore** window displays all of the file systems available for restore. Use ⊞ ☰ to switch between a list view of all file system assets and a hierarchical view of assets within each File System host that has been discovered in PowerProtect Data Manager.
2. Select the check box next to the desired file system, and then click **View Copies**.

   You can also use the **Search** field or the filter in the **Name** column to search on specific criteria to locate a specific file system.

   The **Recovery > Assets** window provides a map view in the left pane and copy details in the right pane.

   When you select a file system in the map view, the file system name appears 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 appear in the right pane.

3. Click **DD**, and then select one of the available copies that appear in the table.
4. In the right pane, select the check box next to the file system backup you want to restore, and then click **Restore**.
   The **Restore** wizard appears.
5. On the **Select Target Location** page, choose from one of the following options, and then click **Next**.
   - **Restore to original**—Restore the file system to the original location.
   - **Restore to a new location on the original hos**t—Select the destination file system asset (volume) from the list of available assets on the host.
   - Restore to a new host—Browse from the available hosts to locate and select a destination host and file system.

   NOTE: If the destination file system asset already contains some data, this data will be overwritten.
6. On the **Summary** page:
   a. Review the information to ensure that the restore details are correct.
   b. Click **Restore**.
7. Go to the **Jobs** window to monitor the restore.
   A restore job appears with a progress bar and start time.

Centralized file-level restore of a file system asset

A file-level restore enables the administrator to recover individual files from backups of file systems that were created in PowerProtect Data Manager.

Prerequisites

Ensure the following for Linux file system hosts:

- You have enabled the SELinux `nis_enabled` parameter by running one of the following relevant commands:
  - RHEL 8.x or CentOS8.x: **`setsebool -P nis_enabled 1`**
  - RHEL 7.x or CentOS7.x: **`setsebool -P nis_enabled 1`**
  - RHEL 6.x or CentOS 6.x: **`setsebool -P allow_ypbind 1`**

  You can also disable SELinux permanently:

  1. Open the `/etc/sysconfig/selinux` file in a text editor.
  2. Change the value of `SELinux=enforcing` from `enforcing` to `disabled`.
  3. Restart the host machine.
  4. Verify the SELinux status by running the `getenforce` command.
- You have installed the `iscsiadm` utility by installing one of the following relevant packages on the Linux client:
  - RHEL or CentOS: iscsi-initiator-utils<version_number>.rpm
  - SLES: open-iscsi<version_number>.rpm
- On SLES, if you want to start the iscsiadm utility for the first time, restart the iSCSI services by running the following command: **`service open-iscsi restart`**
- Review the section Supported platform and OS versions for file system file-level restore for supported platform and operating system versions. PowerProtect Data Manager supports file-level restore only if the backup or replica is on a DD system device.

Steps

1. From the PowerProtect Data Manager UI, go to **Recovery** > **Assets**, and then select the **File Systems** tab.

   The **Restore** window displays the file systems that are available for restore. Use ☷ ≡ to switch between a list view of all file system assets and a hierarchical view of assets within each File System host that has been discovered in PowerProtect Data Manager.
2. Select the check box next to the file system, and then click **View Copies**.

   You can also use the filter in the **Name** column to search for the name of the specific file system or click the **File Search** button to search on specific criteria. See File system file level restore from a search for more information.

   NOTE: The **File Search** is not supported for Linux files.

   The **Restore > Assets** window provides a map view in the left pane and copy details in the right pane.

When a file system is selected in the map view, the file system name appears 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 appear 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 appear in the table.
4. In the right pane, select the check box next to the file system backup you want to restore, and then click **File Level Restore**.
   The **File level restore** wizard appears.
5. On the **Select target host and mount** page, choose from one of the following options, and then click **Mount**.
   - **Restore to Original**.
   - **Restore to Alternate**.

     NOTE: By default, centralized file-level restore operations restore the entire path of selected files and folders to the destination folder. For example, if the file `D:\Folder\file1.txt` is restored to `G:\CFLR`, it is restored as `G:\CFLR\D\Folder\file1.txt` instead of `G:\CFLR\file1.txt`. However, if you select the **Do not retain the upward folder hierarchy while performing recovery** option, only the selected file will be restored not the entire folder hierarchy. For example, if the file `D:\Folder\file1.txt` is restored to `G:\CFLR`, it is restored as `G:\CFLR\file1.txt`.
6. When the mount is complete, click **Next**.
   The **Select folder and files to recover** page appears.
7. On the **Select folder and files to recover** page:
   a. Expand individual folders to browse the original file system backup, and select the objects that you want to restore to the destination file system.

      You can also use the filter in the **Name** column to search for the name of the specific object.

   b. Click **Next**.
      The **Select restore location** page appears.
8. On the **Select restore location** page:
   a. Select the destination drive. Alternatively, choose the **Overwrite files in restore location** option, in which case existing files on the destination drive will be overwritten.

      NOTE:

      If you choose not to overwrite files and the file or folder has the same name as an existing file or folder, the selected file is renamed either before or after the file extension:

      - On Windows, the selected file or folder is renamed before the file extension. For example, `file1.txt` is renamed to `file1-SSID-timestamp.txt`.
      - On Linux, the selected file or folder is renamed after the file extension. For example, `file1.txt` is renamed to `file1.txt-SSID-timestamp`.

   b. Browse the folder structure of the destination file system to select the folder where you want to restore the objects.
   c. Click **Next**.
9. On the **Summary** page:
   a. Review the information to ensure that the restore details are correct.
   b. Click **Finish**.
10. Go to the **Jobs** window to monitor the restore.
    A restore job appears with a progress bar and start time.

File system file level restore from a search

Within the **Restore** window of the PowerProtect Data Manager UI, click the **File Search** button. The **Search Criteria** pane displays to search files based on specific criteria. In the **Search Criteria** pane, enter or select any one or a combination of the following fields. The files that match the search criteria display in the **Results** pane.

Table 9. File search criteria

Search criteria	Description
File Name	Enter the complete or partial name of the file.
File Type	Enter the file type. For example, **`xls`** or **`doc`**.

Table 9. File search criteria (continued)

Search criteria	Description
Size	Enter the minimum or maximum size of the file and select a unit such as KB, MB, GB, or TB.
Folder Path	Enter the complete or partial folder path of the file.
Show Only Files	Move this slider to the right to filter only the files.
File System Name	Select or enter the file system name.
Host Address	Enter or select the name of the file system host.
Last Backup Only	Move this slider to the right to filter the files that are backed up recently.
Backup Date	Enter or select the specific date range to filter the files based on their backup date.
Date Modified	Enter or select the specific date range to filter the files based on their modified date
Date Created	Enter or select the specific date range to filter the files based on their created date.

File Search enables you to restore files from protected file system backup copies to:

- The original file system host
- An alternate file system host

> **NOTE:**
>
> - File search functionality is supported for Windows NTFS file system.
> - File level restore using **File Search** only supports restore of a single file or directory.
> - For file level restores, the files must be restored from a Windows backup to a Windows file system.

File level restore to original file system host using File Search

Use **File Search** in the PowerProtect Data Manager UI to restore files from one copy to the original file system host. Only the Administrator and the Restore Administrator roles can restore data.

Steps

1. From the PowerProtect Data Manager UI, select **Restore** > **Assets**, and then select the **File System** tab.

   The **Restore** window displays all the file systems available for restore.
2. Click **File Search**, and then perform the following:
   a. Select a file system from the **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 file 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. When finished with your selections, click **Restore**.

   The **File System Restore** wizard appears, displaying the **Location** page.
3. On the **Location** page:
   a. Select **Restore to original host**.
   b. 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 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 file system host using File Search

Use **File Search** in the PowerProtect Data Manager UI to restore files from one copy to a new file system. Only the Administrator and the Restore Administrator roles can restore data.

Steps

1. From the PowerProtect Data Manager UI, select **Restore** > **Assets**, and then select the **File System** tab.

   The **Restore** window displays all the file systems available for restore.
2. Click **File Search**, and then perform the following:
   1. Select a file system from the **Name** list.
   2. 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.
   3. In the **Results** pane, select the file 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.
   4. When finished with your selections, click **Restore**.
      The **File System Restore** wizard appears, displaying the **Location** page.
3. On the **Location** page:
   1. Select **Restore to alternate host**.
      The table on the page updates to display the available destination file systems.
   2. Select the file system.
   3. Click **Next**.

   The **Summary** page appears.
4. On the **Summary** page:
   1. Review the information to ensure that the restore details are correct. You can click **Edit** next to certain rows to change the information.
   2. Click **Restore** or **Finish**.
5. Go to the **Jobs** window to monitor the restore.
   A batch file level restore job 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.

Supported platform and OS versions for file system file-level restore

File system file-level restore is only supported for the following platforms and operating systems.

> **NOTE:** Platforms and operating systems are qualified for file-level restore support using the default file system for these platforms:

- RedHat Enterprise Linux
- SuSE Linux Enterprise Server
- CentOS
- Windows

Linux platforms require an ext3, ext4, XFS, or BTRFS file system type.

> **NOTE:** Refer to the E-Lab Navigator for the most up-to-date software compatibility information for PowerProtect Data Manager software and the File System agent.

Enable the File System agent after hostname change

After the hostname of the File System agent host is changed, you must update the lockbox setting for the protection policy.

About this task

Perform the following steps to enable the File System agent operations after the hostname is changed.

Steps

1. Re-register the File System agent with PowerProtect Data Manager:
   - For Linux, run the `install.sh` script from the `agentsvc` directory. For more information, see Install the File System agent on Linux.
   - For Windows, run the `fsagent-19.12.0.0.exe` program, and select **Change** when prompted for the action to perform. For more information, see Install the File System agent on Windows in interactive mode .
2. Delete the existing `agents.clb*` lockbox files in the `C:\Program Files\DPSAPPS\common\lockbox` directory on Windows or the `/opt/dpsapps/fsagent/lockbox` directory on Linux.

   > ⓘ **NOTE:** If the File System agent is installed to a non-default path, delete all of the files in the `lockbox` subdirectory of the installation directory.

3. In the PowerProtect Data Manager UI, configure the lockbox:
   a. In the left navigation pane, select **Protection** > **Protection Policies**.
   b. On the **Protection Policies** page, select the applicable protection policy in the list, and then click **Set Lockbox**.
4. From the protection policy, remove any assets that were protected under the old hostname.

   > ⓘ **NOTE:** Until steps 4 through 6 are followed, any asset that was protected under the old hostname is no longer protected under the new hostname.

5. Run a manual discovery.
6. Add any asset now in an *available* state back to the protection policy.

4

Performing Self-Service Backups and Restores with the File System Agent

Topics:

Performing self-service backups of file systems

A host with the File System agent installed requires a PowerProtect Data Manager server to back up file systems.

To back up file systems manually and use PowerProtect Data Manager, register the host to PowerProtect Data Manager, create a self-service protection policy, and configure the retention policy.

ⓘ **NOTE:** Select **Self-Service Protection** when you create the file systems protection policy in the PowerProtect Data Manager UI.

After a host is registered with PowerProtect Data Manager and assets are added to a self-service protection policy, use the `ddfssv` command to run self-service or manual backups on the host file system assets, as in the following example:

```
ddfssv -l FULL -a DFA_SI_DD_HOST=server_name -a DFA_SI_DD_USER=username -a
DFA_SI_DEVICE_PATH=storage_unit_and_path volume_names
```

where:

-l {**FULL** | **INCR**}

Specifies the type of the backup to perform such as full (`FULL`), or incremental (`INCR`). The default value is `FULL`.

-a "DFA_SI_DD_HOST=*server_name*"

Specifies the IPv4 address for the DD that contains the storage unit to back up the file system assets.

-a "DFA_SI_DD_USER=*username*"

Specifies the protection storage unit username. Example: **`Policy-Protection`**

-a "DFA_SI_DEVICE_PATH=*storage_unit_and_path*"

Specifies the name and the path of the storage unit where you want to direct the backup. Example: **`/PolicyProtection/LVMs/2`**

volume_names

Specifies one or more file system volumes to be backed up. Example: **`F:\ E:\ G:\`**

For more information about how to use the `admin` utility to query the list of backups for an asset, see Using the ddfsadmin utility for file systems.

To perform a self-service backup, use the storage unit and username that was created on the DD system when the policy was created. PowerProtect Data Manager discovers these backups and enables centralized restore operations. You can also perform a manual restore operation.

Performing self-service restore of a file system host

When file systems are protected within a protection policy in PowerProtect Data Manager, you can recover the file system data by using the centralized PowerProtect Data Manager restore functionality, or directly by using the self-service restore feature. The following section describes the procedure for self-service restore of file systems.

Prerequisites for file system restores

Before performing centralized or self-service file system restores:

- Ensure that the target or destination volume is not a system volume.
- Ensure that the **File System agent** is not installed and running on the target volume.
- Ensure that there is sufficient space on the target volume for the restore.

Using the ddfsadmin utility for file systems

The ddfsadmin utility provides the following command line options for file system recovery.

ddfsadmin backup query

Before running the `ddfsrc` command to perform a self-service image-level restore of file systems, you can use the `ddfsadmin backup` command to query a list of all the local and remote backups taken for a particular host, as shown in the following:

ddfsadmin backup query -local -v=*volume name* -t=*time value [h = hour,d = days,w = weeks,m = months]* queries the local record file for listing backups.

ddfsadmin backup query -remote -d=*Protection storage system* -s=*storage unit* -u=*username* -p=*DD password* -c=*hostname* -v=*volume name* -t=*time value [h = hour,d = days,w = weeks,m = months]* queries the record file on the protection storage system for listing backups.

Example usage

ddfsadmin backup query -local -v="C:\\" -t=5 displays a list of local backups in C:\ taken within the last five days.

ddfsadmin sync

This command ensures that the catalogs that are on the local machine and in the DD system are synchronized. The following is the usage for the `ddfsadmin sync` command:

```
sync -local options: Sync local record file with record file on DD
sync -remote options: Sync remote record file with file in the local
options:
  -d=<DD host>: Protection storage system host IP
  -u=<DD username>: Protection storage system username
  -s=<DD device path>: Protection storage system device path
  -p=<DD password>: Protection storage system password.[Optional]
```

Example usage

ddfsadmin sync -local -d *x.x.x.x* -u *username* -s */dev_path*

Self-service image-level restore of file systems

You can perform self-service image-level restores of file systems to the original location by using the `ddfsrc` command. This restore is not supported in the following scenarios:

- When the restore destination is the C:\ volume, which can result in the operating system becoming unavailable.
- When the restore destination is a volume with the File System agent installed.

ⓘ **NOTE:** To perform file system restore to an alternate location, use the centralized restore method in the PowerProtect Data Manager UI, as described in the section Centralized image-level restore of a file system asset.

Before running `ddfsrc`, use the `ddfsadmin backup` command to list the local backups for a particular host and obtain the ID of the save set you want to restore. Using the ddfsadmin utility for file systems provides more information about the `ddfsadmin backup` command.

To restore from a particular backup, specify the ID of the save set as an input to the `ddfsrc` command, as in this example:

ddfsrc -h DFA_SI_DEVICE_PATH=*device path (for example, /fsa2)* -h DFA_SI_DD_HOST=*Protection storage system IPv4 address* -h DFA_SI_DD_USER=*Protection storage system username (for example, sysadmin)* -S 1551407738 -r *file path (for example, /volume1_ext3)* -i y.

where:

-h "DFA_SI_DEVICE_PATH=*<storage_unit_and_path>*"

Specifies the name and the path of the storage unit that contains the backup.

-h "DFA_SI_DD_HOST=*<server_name>*"

Specifies the name of the protection storage system server that contains the backup.

When you have a remote (secondary) protection storage system server that has replicated databases to restore, type the name of the secondary server. A user on the secondary protection storage system server must be in the same group as the primary protection storage system server.

-h "DFA_SI_DD_USER=*<Protection storage system_user>*"

Specifies the protection storage system username.

You must register the hostname and the DD Boost username in the lockbox to enable Microsoft application agent to retrieve the password for the registered user.

Self-service file-level restore of file systems

You can perform self-service file-level restores of file systems using the `ddfsrc` command with the **`-I`** option.

Before starting the command, create a file that contains the list of files to be restored. Provide the location of this file as an input to the **`-I`** option, as shown in the following example.

ddfsrc command with input file specified

ddfsrc -h DFA_SI_DEVICE_PATH=*Protection storage unit* -h DFA_SI_DD_HOST=*Protection storage system IP address* -h DFA_SI_DD_USER=*Protection storage system username* -S *savetime-value* -I *path-of-file-containing-list-of-files-for-restore* -i R -d *destination-path-for-restoring-files*

ⓘ **NOTE:** In this command,

- The parameter `R` renames the file.
- If you replace the parameter `R` with `Y`, the file is overwritten.
- If you use `–g` at the end of the command, only the specified file is restored. Else, the entire directory structure is restored to the destination folder. For example, if the file `D:\Folder\file1.txt` is restored to `G:\CFLR`,
  - Without `–g`, the file is restored to `G:\CFLR\D\Folder\file1.txt`.
  - With `–g`, the file is restored to `G:\CFLR\file1.txt`.

The following steps provide more detail:

1. Use the `ddfsadmin` command to list all the available backups. If you know the save set ID of the backup from which you want to restore, skip this step.

   For example, the following command lists all backups taken in the last 55 days.

   ```
   [root@XXXX ~]# ddfsadmin backup query -local -t=55d
   ```

2. Create an input file that contains the list of files to restore. For example:

   ```
   [root@XXXX ~]# cat flr.txt
   ```

   ```
   /new_ext3/file.txt
   ```

   The `flr.txt` file specifies a single file to restore (`file.txt`).

3. Run the `ddfsrc` command. Ensure that you provide the complete path to the input file that you created.

ⓘ **NOTE:** Do not provide a relative path. If you provide a relative path, the command fails.

For example:

```
ddfsrc -h DFA_SI_DEVICE_PATH=Protection storage unit -h DFA_SI_DD_HOST=Protection storage
system IP address -h DFA_SI_DD_USER=Protection storage system username -S savetime-value
-I /root/flr.txt -d destination-path-for-restoring-files
```

where *savetime-value* is the save set ID identified in step 1.

5

Performing Disaster Recovery with the File System Agent in Windows

Topics:

Disaster recovery limitations

The following limitations apply to performing disaster recovery in the File System agent.

- Disaster-recovery data of clusters does not include critical disks in shared storage. Critical disks must be backed up separately.
- Physical host to virtual host (P2V) BMR of a Hyper-V server to a VMware virtual machine is not supported.

Preparing for disaster recovery

Gathering key information

Before starting a disaster recovery operation, you must gather the following information about the relevant systems:

- File system configuration
- Hard drive configuration
- Device driver information for bare-metal recoveries

Critical volumes in disaster recovery

Critical volumes included in disaster-recovery data are shown when selecting assets to be backed up.

The following volumes are included in disaster-recovery data:

- Any volume that contains operating-system files.
- Any volume that contains a third-party service.
- Any noncritical volume that has a critical volume mounted on it, or any noncritical volume that serves as a parent to a critical volume. In either case, both the parent volume and mounted volume are treated as critical.
- If any of the volumes on a dynamic disk is critical, all volumes on the dynamic disk are considered critical. This is a Microsoft requirement.

Discover the assets to back up

If some application assets are not discovered, you can perform an immediate full discovery of application asset sources by using the on-demand discovery feature in the PowerProtect Data Manager UI.

About this task

To initiate a full discovery of application asset sources, complete the following steps:

Steps

1. From the left pane, select **Infrastructure** > **Asset Sources**.
2. On the **File System** tab, select the agent on which the assets are to be discovered.
3. Click **Discover**.
4. Click **Yes** to continue.

Results

You can view the progress of the discovery from the **Jobs** > **System Jobs** page. When the job completes and the asset is discovered, the **Status** is *Available*.

Create a disaster recovery protection policy

About this task

A disaster recovery protection policy should contain objects to be backed up, which include critical volumes and system-state recovery files.

Steps

1. From the left pane, select **Protection** > **Protection Policies**.
2. Click **Add**.
3. In the **Name** field, type a name for the policy.
4. Ensure that the **File System** option is selected, and then click **Next**.
5. Click **Next**.
6. In the **Assets** pane, select the assets that the policy covers, and click **Next**.
7. If a disaster recovery object was selected in the previous step, leave the **File Exclusions** feature *Disabled*, and then click **Next**.
8. In the **Objectives** pane, click **Next**.
9. In the **Disaster recovery options** pane, select the options that you want applied to the policy, and then click **Next**.
   - **Back up system state files only** - Performs a backup of system state files only. By default, this check box is not selected and bare-metal recovery (BMR) data is backed up.

     NOTE: If the policy is configured with this option, you can only perform a system-state recovery (SSR), and the backed up data will only contain SSR information. BMR with WinPE is not possible.
   - **Ignore missing system state files** - Missing Windows system state files are reported as errors, and the backup fails, reporting the files as missing. This option is selected by default.
   - **Exclude non-critical dynamic disks** - If any volume of a dynamic disk pack is critical, all volumes in the dynamic disk pack are considered critical. By default, this option is not selected and noncritical dynamic disks are included in the backup data. To avoid the creation of large system state files, select this option to exclude noncritical dynamic disks from the backup data.
   - **Ignore third-party services when identifying critical volumes** - When a Windows service or application is installed on an otherwise noncritical disk, that disk is considered critical. By default, this option is not selected and the backup includes the disks on which a Windows service or application is installed. To avoid the creation of large system state files, select this option.
10. Click **Next**.
11. Click **Finish**.

Results

You can view the progress of the policy creation from the **Jobs** > **System Jobs** window.

If you use the **Edit Policy** wizard to add a disaster recovery asset to an existing protection policy, the **Disaster recovery** pane is shown, with options that are the same as the options described in step 9.

Synchronize all clocks

To ensure discovery of all disaster recovery assets, ensure that the clocks on both the host and PowerProtect Data Manager are synchronized to the local Network Time Protocol (NTP) server.

Manually run a disaster recovery policy

Steps

1. From the left pane, select **Protection** > **Protection Policies**.
2. Select the disaster recovery policy that you want to run.
3. Click **Protect Now**.
4. Click **Next**.
5. Select whether you want to back up all assets or a customized set.
6. Click **Next**.
7. In the **Select backup type** drop-down list, select the type of backup that you want.
8. In the **Retain for** fields, specify how long you want the backup kept.
9. Click **Next**.
10. (Optional) To change the assets selected to be backed up or the configuration of the backup data, click **Edit** and make the necessary changes.
11. Click **Protect Now**.

Results

You can view the progress of the backup on the **Jobs** > **Protection Jobs** page.

Performing system-state recovery

System-state recovery (SSR) is an online recovery that enables you to recover an online or powered-on machine that has lost its system files and registry. Perform an SSR when you want to restore certain selected operating system files from a known good backup to replace the corrupted or missing files. You can perform granular recoveries of selected writers from backed up bare-metal recovery (BMR) or SSR data. All the system files in the backup can be recovered only to their original location. Recovering the data to alternate hosts or locations is not supported.

Following are a few examples of files and components that are included in an SSR:

- Boot files
- COM+ class registration database
- Registry and IIS metadata
- Active Directory (NTDS)
- System volume (SYSVOL)

Perform a system-state recovery

If system files or registry entries are lost, you can recover the relevant writers and perform a system-state recovery (SSR).

Prerequisites

- Ensure that the host for which the SSR is to be performed is powered on.
- Ensure that the writers on the host are available and in a stable state.

- When performing an SSR, ensure that there is at least 50% of free space on the system disk.

Steps

1. In PowerProtect Data Manager, from the left pane select **Restore** > **Assets**.
2. Select the check box for the relevant client.
3. Click **View Copies** to view the copies that are backed up.

   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.
4. Select a storage system to display the copies on that storage system.
5. Select the desired backup copy, and then click **System State Restore**. After the backup copy is mounted successfully, a list of backed up writers is displayed.
6. The **Disaster Recovery** asset page selects all writers by default for an SSR. If you deselect individual writers, the following message appears:

   ⓘ **NOTE:** You must select the entire system state to restore. Partial selection of system state restore is not recommended unless it is for Active Directory restore.
7. If you deselected one or more writers and the warning appeared, click **OK**.
8. To start the SSR, click **Finish**.
9. To see the status of the SSR, from the left pane select **Jobs** > **Protection Jobs**.
10. Wait for the SSR to complete.
11. Restart the host for which SSR was performed.

    △ **CAUTION: Failing to restart the host can result in system instability.**

Recovering the Active Directory

When you want to recover the Active Directory specifically, you must choose only NTDS writer and perform an Active Directory (AD) restore .

To recover the Active Directory, perform the following steps:

1. Configure the client. Configure the client to boot into Directory Services Restore Mode (DSRM) provides more information.
2. Recover the Active Directory. Restore Active Directory from the disaster recovery backup provides more information.
3. Perform an authoritative or nonauthoritative Microsoft restore based on user configuration. Authoritative and nonauthoritative restore provides more information.

Configure the client to boot into Directory Services Restore Mode

Before you recover the Active Directory from disaster-recovery data, configure the client to boot into Directory Services Restore Mode (DSRM).

Steps

1. Run the `msconfig` command. The System Configuration window appears.
2. On the **Boot** tab, select **Safe boot**, and then select **Active Directory repair**.
3. Click **OK**.
4. Restart the computer into Directory Services Restore Mode (DSRM).

Recover the Active Directory from disaster-recovery data

About this task

After you have configured the client to boot into Directory Services Restore Mode (DSRM), recover the Active Directory from disaster-recovery data.

Steps

1. Open **PowerProtect Data Manager**.
2. On the **Restore** tab, in the list of clients, select the client that you want to recover.
3. In the drop-down list for the host, select **Disaster Recovery**.
4. Click **View Copies** to view the backed-up copies.
5. Click the storage targets to display the copies.
6. Select the desired backup copy and click **System State Restore**.
7. After the copies are mounted, select the Windows NT Directory Services (NTDS) writer in the Disaster Recovery folder, and then click **Next**.
8. Click **Finish** to start the system-state recovery (SSR).
9. Wait for the Active Directory recovery to complete.
10. Restart the client after the recovery completes.

    ⓘ **NOTE:** After you perform all writer restore (including registry writer) in the Directory Services Restore Mode (DSRM), restart the system in normal mode and perform only registry writer restore to get the user hives (collection of files) restored.

Authoritative and nonauthoritative Microsoft restores

You can perform either a nonauthoritative or an authoritative Microsoft restore of Active Directory.

- Use a nonauthoritative restore when Active Directory replication partners can return a domain controller to a known state. You restore the domain controller from a backup. When you restart the domain controller after the restore, other domain controllers replicate changes made after the backup.
- Use an authoritative restore to return a domain controller to a known state as the master copy. The data from the restored domain controller replicates to other domain controllers. An authoritative restore also enables you to mark specific organizational units (OUs) so that Active Directory objects replicate to other domain controllers. Replication partners do not overwrite the replicated objects.

The following Microsoft TechNet articles provide details on an authoritative restore:

- "Performing Authoritative Restore of Active Directory Objects" provides general details on an authoritative restore.
- "Mark an Object or Objects as Authoritative" provides details on the command syntax for marking items for an authoritative restore.

    ⓘ **NOTE:** Microsoft recommends using a nonauthoritative restore or reinstallation to restore a domain controller. The Microsoft TechNet article "Performing Nonauthoritative Restore of Active Directory Domain Services" provides information about reinstating a domain controller with a nonauthoritative restore.

You can choose whether to perform a nonauthoritative restore or an authoritative restore based on user configuration.

Perform a nonauthoritative Microsoft restore

After the Active Directory recovery completes, restart the client normally. Other domain controllers replicate changes to the client after the restart.

Perform an authoritative Microsoft restore

In an authoritative Microsoft restore, the data from the recovered domain controller replicates to other domain controllers.

Steps

1. Open a command-prompt window and run `ntdsutil` to mark objects for the authoritative restore.

    The objects replicate to other domain controllers during the authoritative restore. In addition, replication partners do not overwrite the replicated objects.

    You can mark a single user object, an entire user subtree, containers, or the entire database. You can use Microsoft `ADSIEdit` to display Distinguished Names for AD objects.

For example, the following series of commands marks a user with an OU of `CN=Test User,CN=Users,DC=svr1,DC=mydomain,DC=com` for an authoritative restore:

```
ntdsutil
        activate instance NTDS
          authoritative restore
          restore object
          “CN=Test User,CN=Users,DC=svr1,DC=mydomain,DC=com”
          quit
         quit
```

The Microsoft documentation provides details on using the **`ntdsutil`** utility for an authoritative restore.

2. If you used Windows System Configuration to configure the system to boot into DSRM, use Windows System Configuration again and clear **Safe boot** to enable the system to boot normally.
3. Restart the client.

Performing bare-metal recovery

Bare-metal recovery (BMR) is used as part of a disaster recovery plan that provides protection when a machine cannot start and you must recover everything. Disaster situations include hardware failure and cyberattacks.

You can use BMR when your host is not available due to a hardware failure or it cannot start. Use BMR for either of the following reasons:

- You want to recover a computer in its entirety after a hardware failure that has been repaired.
- You want to recover data to a new computer after a hardware failure that cannot be repaired. The new computer does not have an operating system, and the OS files must also be recovered from the old computer.

By default, BMR data is System State enabled.

BMR data consists of the following:

- The operating system files and all data except user data on critical volumes

  NOTE: Critical volumes include the boot volume, the system volume, and the volume that hosts system state data, such as Active Directory and application services.
- All system state information

BMR can be used for any of the following operations:

- Physical machine to physical machine (P2P)
- Physical machine to virtual machine (P2V)
- Virtual machine to virtual machine (V2V)

NOTE: P2V BMR of a Hyper-V server to a VMware virtual machine is not supported.

To protect a Windows host entirely, it is recommended that you back up BMR data for critical volumes and separately back up regular assets that contain user data.

Bare-metal recovery requirements

Before you perform bare-metal recovery (BMR), verify that the environment meets the following requirements and that you have the necessary information:

- The hardware on the target host is operational.
- The hardware configuration on the target host is similar to the hardware configuration on the source host from which the BMR data was obtained. Any hardware, driver, or firmware differences between the target and source hosts can cause BMR to fail.
- The size of the disks on the target host is equal to or greater than the size of the disks on the source host. BMR fails to initialize and format a disk when the disk size on the target host is less than the disk size on the source host, even if the target system disk size is sufficient for the BMR data. After the BMR operation, some unallocated space might remain. You can extend the partition size after the BMR operation to use this extra space.
- There are at least as many disks on the target host as there were on the source host. The disk LUN numbering on the target host must match the disk LUN numbering on the source host.
- Both the source and target hosts use 64-bit Windows.

- Both the source and target hosts boot using BIOS or both boot using UEFI.
- For the BMR of a UEFI system, a drive letter is available.
- The source host to be recovered is turned off before the BMR is started.
- A custom WinPE image is available.
- You have the following information available:
  - The IP address and network name of the target host.
  - The network name or IP address of the PowerProtect Data Manager server to use for the BMR operation.
  - Account credentials for the Admin account on the PowerProtect Data Manager server.
  - The source hostname. To obtain the source hostname from the PowerProtect Data Manager UI, select **Infrastructure** > **Asset Sources**. Keep a note of the displayed source hostname. If an incorrect source hostname is provided in the BMR wizard during the BMR operation, the backup copies are not displayed.

About the WinPE image

WinPE enables you to boot with a minimal subset of Windows features, but still access network resources, disks, and other resources from a command prompt. The custom PowerProtect Data Manager WinPE image contains the NIC and disk drivers for the Windows versions that the WinPE image supports.

You can burn the WinPE image to a CD, DVD, or USB flash drive, and then boot the target host from that media.

When you boot with a customized WinPE image, the boot process automatically starts the **PowerProtect Data Manager Bare Metal Recovery Wizard**.

Using a custom WinPE image

PowerProtect Data Manager provides a custom WinPE image that enables you to recover a source host to a target host without installing an operating system. Because local disks are not in use by the operating system, the recovery process can replace files without conflict.

The custom PowerProtect Data Manager WinPE image is based on Windows PE 10.0, and contains the NIC and disk drivers for the Windows versions that the WinPE image supports.

If the custom WinPE image does not contain the drivers for the NIC or disk devices on the source host that you are recovering, you can perform one of the following tasks:

- Copy the drivers to a USB flash drive, and then connect the drive after booting with the custom PowerProtect Data Manager WinPE image.
- Create a WinPE image that includes the drivers, and boot from that image. For more information, see (Optional) Adding NIC or disk drivers to the WinPE ISO file.

The drivers must meet the following requirements:

- 64-bit.
- Do not require a restart during installation.

  NOTE: The WinPE environment loads only in memory, and changes are not persistent across a restart. If a restart prompt appears, you might be able to ignore the prompt. Most NIC drivers are plug-and-play.

Use the custom WinPE image with BMR

About this task

Download, modify, and deploy the custom WinPE image for the BMR of a Windows target computer by completing the following procedure.

Steps

1. Download the custom WinPE image from the PowerProtect Data Manager server. For more information, see Download the custom WinPE image from the PowerProtect Data Manager server.
2. If the WinPE ISO image does not contain the drivers for the NIC or disk devices on the source host that you are recovering, and you do not want to load the drivers from a separate disk during the BMR operation, and then add the drivers to the WinPE image. For more information, see Add NIC or disk drivers to the custom WinPE image.
3. Use one of the following methods to deploy the WinPE image:

- To boot the target host locally, burn the WinPE image to a CD, DVD, or USB flash drive.
- To boot the target host over the network, copy the WinPE image to a Windows Deployment Services (WDS) server. For more information, see Add the custom WinPE image to a Windows Deployment Services server.

Download the custom WinPE image from the PowerProtect Data Manager server

About this task

Complete the following procedure to download the custom WinPE image.

Steps

1. Open a web browser and type the following URL:

   `https://<server>`

   where *<server>* is the DNS name or IP address of the PowerProtect Data Manager server.
2. Select **Settings** > **Downloads**.
3. Select **WinPE**.
4. Click **Download** to download the .iso file of the custom WinPE image.
5. Download the file to a temporary folder.

Add NIC or disk drivers to the custom WinPE image

You can modify the custom WinPE image to add NIC or disk device drivers so you don't have to use a separate disk during the BMR operation.

About this task

If the custom WinPE image does not provide NIC or disk device drivers for the source host, you add them to the image.

NOTE: Modifying the image in any way other than adding NIC or disk device drivers is unsupported.

Steps

1. Open the .iso file of the WinPE image with a utility like UltraISO or MagicISO.
2. Create a folder for the drivers at the top level of the folder structure. The following example creates a `Drivers` folder.

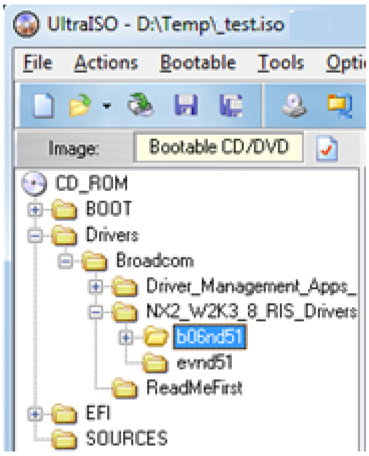

Figure 2. WinPE folders

3. Copy the NIC or disk device drivers to the folder.

   If you have different source hosts that require different NIC or disk device drivers, you can create a subfolder for each device driver.
4. Save the WinPE image with a different name.

Add the custom WinPE image to a Windows Deployment Services server

You can choose to add the custom WinPE image to a Windows Deployment Services (WDS) server to enable the target host to boot over the network. The Microsoft TechNet website provides detailed steps to configure and use WDS.

About this task

ⓘ **NOTE:** WDS is only one method of booting from a WinPE image over the network, but other boot methods are unsupported.

Steps

1. Configure the WDS server.
2. Add the WinPE image to the boot menu.
3. Ensure that PXE booting is enabled on the WDS target host.
4. Boot the target host from the WinPE image over the network.

Perform a bare-metal recovery

About this task

Ensure that the hardware on the target host is operational and that the target host is similar in make, model, and hardware configuration to the source host to be recovered. Also, review the additional requirements in Bare-metal requirements.

⚠ **CAUTION: If the source host to be recovered is powered on, power it down before starting the bare-metal recovery.**

Steps

1. Boot the target host with the custom WinPE image, either locally or over the network.
   The **PowerProtect Data Manager Bare Metal Recovery Wizard** Welcome page is shown.
2. Specify the date, time, and time zone for the host, and then click **Next**.

   If you are restoring to a host in a different time zone or if the system date and time are incorrect, you must change the default date and time.

   ⓘ **NOTE:** If you specify an invalid date or time, the wizard attempts to correct it. Verify that the corrected date and time are accurate.

3. Select the network interface for communication with PowerProtect Data Manager during the BMR operation. If the required NIC driver is not in the list, click **Load Driver** to browse to it.

   ⓘ **NOTE:** The driver must not require a restart. The WinPE environment loads only in memory, and changes are not persistent across a restart. If a restart prompt appears, you might be able to ignore the prompt. Most NIC drivers are plug-and-play.

4. Click **Next**.
   The **Hostname and Network** tab opens.
5. In the **Host name** field, type the hostname of the target host.
6. In the **DNS domain** field, type the domain name of the target host.

   If the host resides in a workgroup instead of a domain, leave the field blank.
7. Select the **IPv4** tab to configure the network to communicate with PowerProtect Data Manager during the BMR operation.
8. In the **TCP/IP Address** section, select the IP address to use:
   - If host IP addresses are assigned automatically, then select **Obtain an IP address automatically (DHCP)**. The network must be configured to support DHCP.
   - If host IP addresses are static, select **Use the following IP** address, and then enter the IP address and the IPv4 subnet mask.
   - If PowerProtect Data Manager is on a different subnet, and then type the default gateway in the **Default gateway** field. Otherwise, leave the field blank.
9. In the **DNS Server** section, specify the DNS server information:

- If you added the PowerProtect Data Manager server hostname and IP address to the hosts file, then leave the default values in the **DNS Server** section.
- If the DNS server name is assigned automatically, select **Obtain DNS server address automatically**.
- If the DNS server IP address is static, select **Use the following DNS server addresses**, and then specify the IP address of the DNS server and any alternate DNS server that exists.

10. Verify the disk configuration, and then click **Next**.

    ⓘ **NOTE:** The disk size and number of hard disks that are added to the target machine should be either equal to or greater than that of the source machine.

11. Add the PowerProtect Data Manager server details, and then click **Next**.

    ⓘ **NOTE:**

    - In **Server Name or IP**, enter only the FQDN or IP of the server.
    - It is recommended that you use the Administrator role while providing PowerProtect Data Manager details. If the Restore Administrator role is used, a prompt to enter Data Domain credentials appears.

12. On the **Select Backup** page, select the BMR data to restore to the host. Backups appear in the list in descending order from the most recent to the oldest.
13. Click **Next**.
    A message is displayed while the information to complete the BMR operation is retrieved. Wait while the information is retrieved.
14. To add custom BMR options, click **Options** next to **Custom restore options**.
15. Perform one of the following actions:

    △ **CAUTION: If the Restore physical machine to virtual machine (P2V) option appears during the BMR wizard, select it. If you do not select it, the BMR operation succeeds, but the target host boots with a blue screen. For more information, see Recover from a blue screen on boot after a BMR restore.**

    - To accept the default PowerProtect Data Manager BMR options, click **Restore**.
    - To specify non-default PowerProtect Data Manager BMR options, which are generally used for troubleshooting with assistance from Customer Support, perform these actions:
        a. Click **Options**.
        b. In the **Additional Options** field, type the options and values.

           ⓘ **NOTE:**

           ○ By default, for BMR restore the noncritical disks are not formatted. However, if you need to format any noncritical disks, you can use `-h DFA_SI_EXCLUDE_NON_CRITICAL_DYNAMIC_DISK=FALSE`. The default flag value of the `DFA_SI_EXCLUDE_NON_CRITICAL_DYNAMIC_DISK` additional option is set to `TRUE`.

           ○ Additional options must follow these guidelines:

             ■ Include a space between command and switch.

             ■ A key value pair should not contain any white space, for example,

             `-h DFA_SI=TRUE -h DFA_SI_DR_P2V=TRUE`.

        c. Click **OK**.
        d. To confirm that you want to format the data and continue the BMR operation, click **OK**.
        e. Perform one of the following actions:
           ○ To cancel the BMR operation, click **Cancel**.
           ○ To proceed with the BMR operation, click **Restore**.

16. If you clicked **Restore**, wait until the BMR operation is successful.

    ⓘ **NOTE:** The wizard takes approximately 30 seconds to update the status (Cancelled, Failed, or Successful) in PowerProtect Data Manager.

To monitor the status of the BMR job from the PowerProtect Data Manager UI, select **Jobs** > **Protection Jobs**.

Next steps

Consider the following after the BMR operation is complete:

- The final status of the BMR operation is displayed on the **Results** tab.
- To open the BMR logs, click **View Logs**.
- To open a specific BMR log, select it, and then click **Open**.
- If the status of the recovery is **Cancelled** or **Failed**, restart the target host or boot it with the custom WinPE image again.
- If the virtual machine that was recovered boots using UEFI, the following error message appears in the `ddfsrc` log file: `Virtual Disk Service error: This disk is already online.` This message can be ignored.

Saving bare-metal recovery logs

The BMR logs might be needed for troubleshooting purposes. However, the WinPE environment does not allow copy, paste, or remote desktop connections.

About this task

To save the logs after the BMR operation completes, perform the following steps.

⚠ CAUTION: **If the target host is restarted, the logs are lost.**

Steps

1. If not already open, open a command-line window.
2. Mount a shared drive location to which you intend to copy the logs by running the following command:

   ```
   net use s:\<share-ip-address\sharename> /user:<username> <password>
   ```

3. Run `cd X:\Program Files\DPSAPPS\fsagent\logs`.
4. Copy the files or folder to the mounted shared drive by running the following command:

   ```
   copy ddfsrc.log s:\<name of destination folder on shared drive>
   ```

Results

ⓘ **NOTE:** You can also run `notepad.exe` to open the logs and see them in the WinPE environment.

Recover from a blue screen on boot after BMR

If you are performing a physical-to-virtual (P2V) operation with the **PowerProtect Data Manager Bare Metal Recovery Wizard**, the **Restore physical host to virtual host (P2V)** option might appear. If you do not select it, BMR succeeds but the target host boots with a blue screen.

About this task

In rare circumstances, network connectivity issues can prevent the BMR wizard from detecting if a target host is virtual or physical. If no confirmation is given, certain registry entries are not modified to the values required for a virtual host.

To correct the situation, perform the following actions:

Steps

1. Boot the target host with the WinPE image.
2. From the command-line window, run `diskpart` and `list volumes` to identify the current drive letter for the original system drive.
3. Run `ddfsrc.exe -h DFA_SI_DR_PATCH_REG_PATH="C:\Windows"`, replacing *C:* with the drive letter obtained in step 2.
4. Restart the host.

Next steps

The target host boots without a blue screen.

Perform bare-metal recovery of Windows clusters

Bare-metal recovery (BMR) can restore a Windows cluster configuration. BMR restores only the system state and critical disks on the cluster nodes.

Prerequisites

- The shared disk data and user data are protected using the relevant application agents.
- The hardware configuration of the cluster-node Windows clients is recorded. Necessary information includes the hardware vendor, size and type of disks, type of NIC, and amount of memory assigned.

About this task

To restore the system state and critical disks on the cluster nodes, perform the following steps.

Steps

1. If the old cluster-node Windows clients are powered on, power them off.
2. Create two new Windows clients with the same hardware configuration as the old cluster-node Windows clients.
3. Perform BMR on both of the new Windows clients.
4. Power on the Windows clients.
5. Open the Failover Cluster Manager and wait for the cluster to be connected.
6. Open Disk Management and initialize the new critical disks with the same configuration and labels as the old critical disks.
7. For each non-Cluster Shared Volume disk, perform the following substeps:
   a. Perform a file-system restore.
   b. Select the disk, and then click **More Actions** > **Repair**, replacing the disk.
   c. Select the disk, and then click **Bring Online**.
8. Refresh the cluster node and confirm that all non-Cluster Shared Volume disks are online.
9. In the Failover Cluster Manager, perform the following substeps for each Cluster Shared Volume:
   a. Record its name.
   b. Remove it.
10. For each Cluster Shared Volume disk, perform the following substeps:
    a. Select the disk, and then click **More Actions** > **Repair**, replacing the disk.
    b. Perform a file-system restore for each Cluster Shared Volume, using the name recorded in step 9.
    c. Select the disk, and then click **Bring Online**.
11. Refresh the cluster node and confirm that all Cluster Shared Volume disks are online.

Next steps

Use normal File System agent backups to restore file system data, noncritical disks, and critical disks on shared storage. Also, use application-agent backups to restore application data.

Disaster recovery solution for Microsoft SQL application data

This section provides an end-to-end Disaster Recovery (DR) solution for Microsoft SQL application data in Microsoft Windows. This solution requires Microsoft SQL Server application and File System agents on Windows.

File System agent on Windows (FSA-BMR) protects Windows System data (critical volumes) and, the Microsoft SQL Server application agent protects the Microsoft SQL Server System and user databases. This scope of protection derives from Microsoft.

In detail, the volumes, where Microsoft SQL Server is installed and configured are considered as critical volumes. The FSA-BMR protects only the Windows critical volumes, which include Windows System Partition and any other volumes, where the third-party application or service is installed. Also, through FSA-BMR, the Windows System data, SQL installation, and configuration data are protected. The Microsoft SQL Server application agent protects the Microsoft SQL Server system database and user-created databases.

Protecting Windows system data and its critical volumes

Install and configure the File System agent on Windows to protect the Windows System data and critical volumes. See Critical volumes in disaster recovery for more information about the steps to configure and protect Windows system data.

Protecting Microsoft Server SQL application data

Install and configure the Microsoft SQL Server application agent to protect the Microsoft SQL Server system and user database. See *PowerProtect Data Manager Microsoft SQL Server User Guide* for more information about the steps to configure and protect the Microsoft SQL Server system and user database.

Performing DR for Microsoft SQL application data

The Microsoft SQL Server application agent needs a Microsoft SQL Server service to be running in single-user mode to restore the system database (master database). Since the File System agent on Windows does not backup the SQL server system database, the user needs to perform the below steps for an end-to-end DR solution for the SQL system database and user database in Windows.

About this task

See Microsoft documentation and *PowerProtect Data Manager Microsoft SQL Server User Guide* for more information on the following procedure.

Steps

1. Perform the BMR restore of Windows. See Performing bare-metal recoveryfor more information.
2. Mount the Microsoft SQL Server installation media in Microsoft Windows and run the following command. This rebuilds the Microsoft SQL Server System database.

   ```
   Setup /QUIET /ACTION=REBUILDDATABASE /INSTANCENAME=MSSQLSERVER_2017 /
   SQLSYSADMINACCOUNTS=bmrtestdomain\administrator /SAPWD=Password
   ```

   NOTE: Select the Microsoft SQL Server version according to the SQL version instance installed and configured. The above command was for the Microsoft SQL Server version 2017.

3. Start the Microsoft SQL Server instance in single-user mode and using the Microsoft SQL Server application agent, restore the Microsoft SQL server system database (master database). There are many ways, the user can start the Microsoft SQL Server instance in single-user mode. Perform the following steps to configure Microsoft SQL Server 2017 instance in a single-user mode.
   a. Start the SQL Server Configuration Manager.
   b. Right-click on the SQL server instance and select **Properties**.
   c. In the **Startup parameters** tab, enter **-m** in the **Specify a startup parameter** field and click **Add**.
   d. Click **Apply** and **Ok**.
   e. Restart the SQL server instance.

   The following example describes restoring the System DB through CLI:

   ```
   C:\Program Files\DPSAPPS\MSAPPAGENT\bin>ddbmsqlrc.exe  -a
   NSR_DFA_SI_DD_HOST=192.162.1.1 -a NSR_DFA_SI_DD_USER=PLC_SQL_62-ppdm1461-f1cad
   -a NSR_DFA_SI_DEVICE_PATH=/PLC_SQL_62-ppdm1461-f1cad/PLCTLP-fddae07f-d1c3-497e-8b7c-
   a8d90f270812 -a "NSR_DFA_SI_DD_LOCKBOX_PATH=C:\Program Files\DPSAPPS\common\lockbox"
   -c bmrtestvm-62.bmrtestdomain.com -a "SKIP_CLIENT_RESOLUTION=TRUE" -f -t "06/03/2022
   08:08:36 PM" -S normal MSSQL$MSSQLSERVER_2017:master
   ```

4. Start the Microsoft SQL Server instance in multiuser mode. Use the Microsoft SQL Server application agent to restore the msdb and model database.
   a. Start the SQL Server Configuration Manager.
   b. Right-click on the SQL server instance and select **Properties**.
   c. In the **Startup parameters** tab, select **-m** from the **Existing parameters** field and click **Remove**.
   d. Click **Apply** and **Ok**.

e. Restart the SQL server instance.

See *PowerProtect Data Manager Microsoft SQL Server User Guide* follow the steps to recover the Microsoft SQL Server msdb and model database.

The following example describes restoring the msdb database through CLI:

```
ddbmsqlrc.exe  -a NSR_DFA_SI_DD_HOST=192.168.1.1 -a NSR_DFA_SI_DD_USER=PLC_SQL_62-
ppdm1461-f1cad -a NSR_DFA_SI_DEVICE_PATH=/PLC_SQL_62-ppdm1461-f1cad/PLCTLP-fddae07f-
d1c3-497e-8b7c-a8d90f270812 -a "NSR_DFA_SI_DD_LOCKBOX_PATH=C:\Program
Files\DPSAPPS\common\lockbox" -c bmrtestvm-62.bmrtestdomain.com -a
"SKIP_CLIENT_RESOLUTION=TRUE" -f -t "06/03/2022 08:08:36 PM" -S normal
MSSQL$MSSQLSERVER_2017:msdb
```

The following example describes restoring the model database through CLI:

```
ddbmsqlrc.exe  -a NSR_DFA_SI_DD_HOST=192.168.1.1 -a NSR_DFA_SI_DD_USER=PLC_SQL_62-
ppdm1461-f1cad -a NSR_DFA_SI_DEVICE_PATH=/PLC_SQL_62-ppdm1461-f1cad/PLCTLP-fddae07f-
d1c3-497e-8b7c-a8d90f270812 -a "NSR_DFA_SI_DD_LOCKBOX_PATH=C:\Program
Files\DPSAPPS\common\lockbox" -c bmrtestvm-62.bmrtestdomain.com -a
"SKIP_CLIENT_RESOLUTION=TRUE" -f -t "06/03/2022 08:08:36 PM" -S normal
MSSQL$MSSQLSERVER_2017:model
```

5. Restore the user database using the Microsoft SQL Server application agent.

   See *PowerProtect Data Manager Microsoft SQL Server User Guide* follow the steps to recover the Microsoft SQL Server user database.

Protecting Microsoft Distributed File System using BMR and SSR

Bare-metal recovery (BMR) and system-state recovery (SSR) are responsible for protecting the Microsoft Distributed File System (DFS) metadata/namespaces.

DFS data can be categorized into,

- DFS metadata (DFS namespace)
- DFS user data (user data share linked to DFS links)

Depending on the DFS configuration type (stand-alone or domain-based DFS), DFS stores its metadata in various locations such as registry, active directory, and so on.

BMR backup

If DFS links and DFS user data share are part of critical volumes, BMR backups them. See Critical volumes in disaster recovery for more information.

BMR restore

If DFS links and DFS user data are part of critical volumes, by default, BMR restores them including all the DFS metadata.

SSR backup

SSR backups only the DFS config data but not the DFS user data.

SSR restore

Always perform the full system state restore to fetch the DFS metadata information. If the DFS machine is a domain-based appliance, perform the full system state restore followed by AD authoritative restore.

NOTE: Performing full system state restore helps in completing the restore process even when DFS service files are corrupted.

To protect DFS user data,

- Use File System agent to protect user data.
- If the user data is present on NAS share, use NAS agent to protect it.
- If the user data is part DFS other than File System or NAS agents, use the respective agent to protect it.

Performing application restores after bare-metal recovery

Some applications are not recovered by BMR.

When you back up BMR data, the backups include binaries for applications that use Windows services, such as Microsoft SQL. However, the backups normally exclude binaries for applications that do not use Windows services, as well as their configuration, databases, and file.

You need to reinstall the following applications and their data, or restore them from a File System agent backup:

- Applications that do not use Windows services.
- Applications installed to a noncritical volume that has been destroyed.

To restore application data, use the relevant application agent backup.

6

Performing Self-Service Backups and Restores for Disaster Recovery

Topics:

Performing self-service backups for disaster recovery

A host with the File System agent installed requires a PowerProtect Data Manager server for disaster recovery asset.

To back up file systems manually and use PowerProtect Data Manager, register the host to PowerProtect Data Manager, create a self-service protection policy, and configure the retention policy.

> **NOTE:** Select **Self-Service Protection** when you create the file systems protection policy in the PowerProtect Data Manager UI.

After a host is registered with PowerProtect Data Manager and assets are added to a self-service protection policy, use the `ddfssv` command to run self-service manual backups on the host disaster recovery asset, as in the following example:

```
ddfssv -l FULL -a DFA_SI_DD_HOST=server_name -a DFA_SI_DD_USER=username -a
DFA_SI_DEVICE_PATH=storage_unit_and_path volume_names
```

where:

-l {**FULL** | **INCR**}

Specifies the type of the backup to perform such as full (`FULL`), or incremental (`INCR`). The default value is `FULL`.

-a "DFA_SI_DD_HOST=*server_name*"

Specifies the IPv4 address for the DD that contains the storage unit to back up the file system assets.

-a "DFA_SI_DD_USER=*username*"

Specifies the protection storage unit username. Example: **`Policy-Protection`**

-a "DFA_SI_DEVICE_PATH=*storage_unit_and_path*"

Specifies the name and the path of the storage unit where you want to direct the backup. Example: **`/plc_self_service_protectionpolicy/PLCTLP-ab31adac-1a4f-4d26-9d00-a3148d63805a`**

-a "DFA_SI_DR_SSRONLY=*TRUE*"

Specifies whether the SSR needs to backed up or not. Set the flag value to **`TRUE`** if you want to perform SSR backup. The default value of this flag is **`FALSE`**. This is optional for BMR backups.

-a "DFA_SI_IGNORE_MISSING_VSS_FILES= *TRUE*"

Specifies whether the missing windows system state files must be ignored during the self-service backup. The default value of this flag is **`TRUE`**. This flag states that the backup is completed successfully instead of stating the backup is completed with exceptions. However, the corresponding logs list the missing files as warnings.

> **NOTE:** If the flag value of this command is set to **`FALSE`**, the missing files will be listed as errors in logs and the backup is completed with exception.

volume_names

Specifies Disaster Recovery Asset to be backed up. Example: **`DISASTER_RECOVERY:\\`**

For more information about how to use the `admin` utility to query the list of backups for an asset, see Using the ddfsadmin utility for disaster recovery.

To perform a self-service backup, use the storage unit and username that was created on the DD system when the policy was created. PowerProtect Data Manager discovers these backups and enables centralized restore operations. You can also perform a manual restore operation.

Using the ddfsadmin utility for disaster recovery

The ddfsadmin utility provides the following command line options for disaster recovery asset.

ddfsadmin backup query

Before running the `ddfsrc` command to perform a self-service system state restore for disaster recovery asset, you can use the `ddfsadmin backup` command to query a list of all the local and remote backups taken for a particular host, as shown in the following:

ddfsadmin backup query -local -t=*time value [h = hour,d = days,w = weeks,m = months]* queries the local record file for listing backups.

Example usage

ddfsadmin backup query -local -t=5d displays a list of local backups in **DISASTER_RECOVERY:\\** taken within the last five days.

ddfsadmin sync

This command ensures that the catalogs that are on the local machine and in the DD system are synchronized. The following is the usage for the `ddfsadmin sync` command:

ddfsadmin sync -local -d *x.x.x.x* -u *username* -s */dev_path*

```
options:
  -d=<DD host>: Protection storage system host IP
  -u=<DD username>: Protection storage system username
  -s=<DD device path>: Protection storage system device path
  -p=<DD password>: Protection storage system password.[Optional]
```

Self-service system state restore for disaster recovery

You can perform self-service system state restores for disaster recovery asset using the `ddfsrc` command with the **-I** option.

Before starting the command, create a file that contains the list of writers to be restored. Provide the location of this file as an input to the **-I** option, as shown in the following example.

ddfsrc command with input file specified

ddfsrc -h DFA_SI_DD_HOST=*Protection storage system IP address* -h DFA_SI_DD_USER=*Protection storage system username* -h DFA_SI_DEVICE_PATH=*Protection storage unit* -h DFA_SI_DR_SSRONLY=TRUE -I *path-of-file-containing-list-of-writers-to-restore* -S *savetime-value*

where:

-a "DFA_SI_DD_HOST=*server_name*"

Specifies the name of the protection storage system server that contains the backup. When you have a remote (secondary) protection storage system server that has replicated databases to restore, type the name of the secondary server. A user on the secondary protection storage system server must be in the same group as the primary protection storage system server.

-a "DFA_SI_DD_USER=*protection_storage_system_user*"

Specifies the protection storage system username. You must register the hostname and the DD Boost username in the lockbox to enable Microsoft application agent to retrieve the password for the registered user.

-a "DFA_SI_DEVICE_PATH= *storage_unit_and_path*"

Specifies the name and the path of the storage unit that contains the backup.

-a " DFA_SI_DR_SSRONLY=*TRUE*"

Specifies the flag status to TRUE if you want to perform SSR restore. The default flag value is FALSE.

-I "*path-of-file-containing-list-of-writers-to-restore*"

Specifies the path of the file containing the list of writers to be restored.

-S "*savetime-value*"

Specifies the save set ID of a backup copy which needs to be restored.

The following steps provide more detail:

1. Use the `ddfsadmin` command to list all the available backups. If you know the save set ID of the backup from which you want to restore, skip this step.

   For example, the following command lists all backups that are taken in the last 55 days.

   ```
   ddfsadmin backup query -local -t=55d
   ```

2. Create an input file that contains the list of writers to restore. For example:

   ```
   Notepad.exe ssr.txt
   ```

   - The `ssr.txt` file specifies a single writer to restore. For example, **`System Writer`**

     or

   - The `ssr.txt` file specifies multiple writers that must be restored, where each writer name should be specified in new line. For example,

     ```
     System Writer
     Registry Writer
     Task Scheduler Writer
     WMI Writer
     ```

3. Run the `ddfsrc` command. Ensure that you provide the path to **`ssr.txt`** file that you created.

   For example:

   ```
   ddfsrc -h DFA_SI_DD_HOST=Protection storage system IP address -h
   DFA_SI_DD_USER=Protection storage system username -h DFA_SI_DEVICE_PATH=Protection
   storage unit -h DFA_SI_DR_SSRONLY=TRUE -I C:\\ssr.txt -S savetime-value
   ```

   where *savetime-value* is the save set ID identified in step 1.

Bare metal recovery restore for disaster recovery

You can perform bare metal recovery restore for disaster recovery asset through WinPE.

See Perform a bare-metal recovery for more information.

A

File System Best Practices and Troubleshooting

Topics:

Installation and operation

You might encounter the following issues while installing or operating the File System agent.

Agent registration

On Windows, if the agent fails to establish a connection with the PowerProtect Data Manager server, agent registration might fail with the following error message:

```
During a network connectivity test, the agent is unable to reach the PowerProtect Data
Manager server by using ping.

1.    If the ping command is blocked in the environment, the agent registration can
still complete successfully.
Review the agent service logs at INSTALL_DIR\DPSAPPS\AgentService\logs to verify that
the registration is successful. If the registration is successful, the status of the
agent host indicates Registered in the PowerProtect Data Manager UI.
2.    If the ping command is not blocked in the environment, the agent registration
might not complete successfully because a network connection cannot be started. If this
occurs, complete the following steps to troubleshoot the issue:
```

On Linux or AIX, if the agent fails to establish a connection with the PowerProtect Data Manager server, agent registration might fail with the following error message:

```
During a network connectivity test, the agent is unable to reach the PowerProtect Data
Manager server by using ping and curl.

1.    If the ping command is blocked in the environment and curl is not installed, the
agent registration can still complete successfully.
Review the agent service logs at /opt/dpsapps/agentsvc/logs to verify that the
registration is successful. If the registration is successful, the status of the agent
host indicates Registered in the PowerProtect Data Manager UI.
2.    If the ping command is not blocked in the environment, the agent registration
might not complete successfully because a network connection cannot be started. If this
occurs, complete the following steps to troubleshoot the issue:
```

If agent registration fails with these error messages, complete the following operation:

1. Use any network packet tracing tool to trace the packets from the agent system to PowerProtect Data Manager.
2. Start the packet tracing between the source IP of the agent system and the destination IP of PowerProtect Data Manager.
3. Start the network traffic between the agent system and PowerProtect Data Manager.

   Wait 10 to 15 seconds.

4. Analyze the captured packets.

5. Look for SYN and SYN_ACK packets to see if a 3-way handshake is being performed.

   Determine whether the source agent or the destination PowerProtect Data Manager is blocking the connection.

   If network traffic is blocked, contact your network security team to resolve the port communication issue.

PowerProtect agent service operations

To troubleshoot PowerProtect agent service operations, you can check the PowerProtect 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.

To modify the log level and retention of temporary files, you can perform the following steps:

1. Stop the agent service.
2. Open the `config.yml` file in an editor.
3. Modify the log-level settings in the following parameters, as required:
   - `DEBUG`
   - `INFO`
   - `WARNING`
   - `ERROR`
   - `CRITICAL`

   NOTE: These parameters are listed in order of decreasing number of messages in the debug information output. The default log-level is `INFO`.
4. To retain the temporary files, set the `keepTempFiles` parameter to True in the `config.yml` file.

   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.

PowerProtect Data Manager UI display of localhost.localdomain hostname

In the PowerProtect Data Manager UI, the **Application Agents**, **Asset Sources**, and **Protection Jobs** windows might list the asset primary hostname as localhost.localdomain instead of the expected FQDN.

The display of localhost.localdomain as the hostname in the PowerProtect Data Manager UI windows might occur when you specify the host's actual FQDN setting for the loopback address in the `/etc/hosts` file. For example, when you add the following settings in the `/etc/hosts` file, the first setting value, localhost.localdomain, appears as the hostname in the PowerProtect Data Manager UI windows, instead of the actual FQDN:

```
127.0.0.1 localhost.localdomain localhost6 localhost6.localdomain6
127.0.0.1 blrv027d233.blr.lab.emc.com blrv027d233
```

Ensure that the host's actual FQDN is not specified for the loopback address and do not specify hostnames that start with "local" in the `/etc/hosts` file.

Backups

You might encounter the following issues while performing backups with the File System agent.

Backing up Windows ACL properties

On a Windows client, if the contents of a file have not changed since the last backup but the Access Control List (ACL) properties have, incremental backups will not back up the changed ACL properties.

Perform the following steps to back up the changed ACL information:

1. Enable Last Access from the client by running the command `fsutil behavior set disablelastaccess 0`.
2. Restart the client.
3. Check the status by running `fsutil behavior query disablelastaccess` and looking for `DisableLastAccess = 0` in the output.
4. Set the detect-acl-changes flag to true. The value of this flag is false by default. Edit the `C:\Program Files\DPSFSAGENT\settings\.ddfssv.fsagentconfig` file and change "--detect-acl-changes=true" to set the flag.

Take note of the following:

- When the `--detect-acl-changes` flag is set, the file is treated as a modified file and is backed up as part of the next backup.
- If ACL modifications are made only to executable files residing on a mounted volume, the changes might not be backed up.
- This works only for files, not folders. Changes only to the ACL properties of folders cannot be backed up.

Backups fail when credentials include a backslash character (\)

When you enter credentials that include a backslash character (\) for an application agent in the PowerProtect Data Manager UI, the backups fail.

For example, when you enter a password for the operating system or database user that includes the backslash character, subsequent backups fail with the following error message:

```
systemErr: Unable to log in.
```

This error might occur when updating the password for a storage unit.

To resolve this issue, type \\ (double backslash) instead of \ (single backslash) when you enter the credentials for an application agent in the PowerProtect Data Manager user interface.

Block-based backup driver installation

The following message might appear during the installation of the block-based backup driver: `Block based backup driver was installed but not loaded.` If the driver cannot be loaded, file-based backups will be performed instead of block-based backups.

Perform the following troubleshooting steps in order. Unless otherwise noted, if you make a change at any step, test block-based backups again before proceeding to the next step:

1. If the `bc` utility is not installed, install the utility.
2. If the `livepatch` module is installed and enabled, disable it.
3. Install or reinstall the block-based driver `ppdm-bbbwt`.
4. Restart the `nsrbbb` service. For information on the specific commands to execute, refer to the documentation of the host's operating system.

ⓘ **NOTE:** If you are unable to resolve the issue, contact Customer Support.

Linux block-based incremental backups fail

On Linux, the block-based incremental backups consistently fail and display a message similar to `save: Block Based Error subsystem error while performing Block Based Backup`.

Check if any other process is already accessing the snapshot or delete the snapshot manually, and then try again.

Disaster recovery

You might encounter the following issues while performing disaster recovery with the File System agent.

BMR and SSR operations fail to run and a `start_subscriber` error appears in the agent-service log

A BMR or SSR operation might fail to display the start or completion of a job, and the `DPSAPPS\AgetService` log shows an error similar to `msg_server.py-create_subscriber()Line 617 Exception occurred during start_subscriber Permission denied occurred.`

This is caused when another service uses port 7010 or 7011.

Reconfigure any service that uses port 7010 or 7011 to use a different port.

Backing up BMR data fails with a `ddfssv` error

Backing up BMR data can fail with the error `ddfssv FATAL <12128: Attempt to create a backup with no data is unsuccesful.`

The Event Viewer system log might also contain an error similar to the following:

`The shadow copies of volume H: were deleted because the shadow copy storage could not grow in time. Consider reducing the IO load on the system or choose a shadow copy storage volume that is not being shadow copied.`

This is a known Microsoft issue that affects all backup products.

Retry the backup procedure after leaving more free space on the drive or when the drive is not as busy.

Network connectivity issues after a BMR

A BMR can fail to recover network configuration information such as IP address, subnet mask, gateway, and DNS. If the recovered host experiences network connectivity issues, confirm its network configuration and make any necessary changes.

SSRs fail to restore a VSS writer

If an SSR fails to recover a VSS writer, you might see an error similar to the following:

```
ddfsrc Error <0000>: Unable to select W component from V for restore: The specified
object was not found. (VSS error 0x80042308)
```

This occurs when writer .xml files are missing from the `C:\Windows\Vss\Writers\System` directory.

Restart the host, run the command `vssadmin list writers` to confirm the VSS writer status, and then retry the SSR.

BMR recovers critical volumes, but a disk is marked as offline

This can happen with disks that host Microsoft SQL Server instances.

Manually bring the disk online, and then restart the host.

SSRs show a `RegSetValueEx()` error and fail to recover files after a restart.

An SSR might show `Error <10958>: RegSetValueEx() for replace files`, but complete successfully. After the host is restarted, certain files have not been recovered.

A file that is in use cannot be replaced by its recovered version. If you restart a host to have a file replaced but the file is not replaced, it might be because antivirus software is preventing access to the *pendingfilerenameoperations* registry key.

Perform one of the following tasks as a workaround.

- Use file exclusion:
    1. Retry the SSR, but do not restart the host.
    2. Exclude `ddfssv.exe`, `ddfsrc.exe`, `ddfscon.exe`, and `restserver.exe` from the antivirus software.
    3. Restart the host.
    4. Optionally, remove the files from the exclusion list.
- Temporarily disable the antivirus software:
    1. Retry the SSR, but do not restart the host.
    2. Disconnect the host from the network.
    3. Disable the antivirus software.
    4. Restart the host.
    5. Enable the antivirus software.
    6. Connect the host to the network.

Temporary files can be deleted manually after a recovery operation

The temporary files that are generated during the recovery operation are stored in `C:\dbapps_temp_dir`. You can delete these temporary files manually after the recovery operation and the reboot.

NOTE:

- Replace *C:* with the drive to which Windows is installed.
- You may require special permissions to delete some temporary files. To delete such files, contact Customer Support.

BMR restore errors

When performing a BMR restore, you might see the errors similar to the following:

```
Assigning volume letters or mount points failed.
```

```
Unable to do VSS restore: Bare metal recovery remount volumes step failed.
```

Perform the BMR restore again.

Cluster assets backup failure

The cluster assets backup fails when there is a combination of either stand-alone and cluster assets, or disaster recovery and cluster assets in the same policy.

Workaround is to run the cluster backup in a different policy and schedule.

BMR backup fails on EFI based system for a few times when backing up the BCD files

Backup for Extensible Firmware Interface (EFI) partition is performed from the live volume as the snapshot volume of the EFI partition cannot be created. If the system process uses the Boot Configuration Data (BCD) files, the ddfssv process tries to export a temporary copy for BCD files using the Microsoft bcdutil tool. This issue occurs if the export operation causes any change in the exported file.

A sample ddfssv log file with errors:

```
--------------------------------------------------------

2022-05-18T08:10:08.914Z
[TRACE_ID:a559c76a1e886397;JOB_ID:9333c654df01e5af;EXEC_ID:af0c561e68d3aa75] ddfssv Info
```

```
<0000>: Exported bcd file to temporary location
2022-05-18T08:10:08.920Z
[TRACE_ID:a559c76a1e886397;JOB_ID:9333c654df01e5af;EXEC_ID:af0c561e68d3aa75] ddfssv
Error <16507>: Path \\?\GLOBALROOT\Device\HarddiskVolume2\EFI\Microsoft\Boot\BCD: Total
processed bytes 32768 is inconsistent with original data size xxxxx
2022-05-18T08:10:08.926Z
[TRACE_ID:a559c76a1e886397;JOB_ID:9333c654df01e5af;EXEC_ID:af0c561e68d3aa75] ddfssv
Error <16507>: Path \\?\GLOBALROOT\Device\HarddiskVolume2\EFI\Microsoft\Boot\BCD.LOG:
Total processed bytes 32768 is inconsistent with original data size xxxxx
...

2022-05-18T10:51:25.078Z [TRACE_ID_a559c76a1e886397_EXEC_ID_af0c561e68d3aa75] ddfssv
Info <6149>: Error summary: 2 errors: 16507(2)
2022-05-18T10:51:25.102Z [TRACE_ID_a559c76a1e886397_EXEC_ID_af0c561e68d3aa75] ddfssv
Info <5314>: Command completed with exceptions (2 errors, exit code 10020: completed
with errors, client log should be examined)
...
------------------------------------------------------------
```

Workaround is to rerun the backup.

IPv6 configuration fails in WinPE

When the user modifies the IPv6 address during the host configuration in the WinPE wizard, the system adds and lists all the IPv6 addresses rather than replacing the existing IPv6 address.

Workaround is to restart the restore process.

Restores

You might encounter the following issues while performing restores with the File System agent.

File-level restores of symbolic-linked directories

The file-level restore of a symbolic-linked directory does not contain any symbolic links or reparse points, but the contents are the same as the source directory.

Create symbolic links manually after the file-level restore operation completes.

File-level restore operations fail with a client services error

When performing a file-level restore, you might see an error similar to one of the following:

```
Resource not found. Check if client services are running and perform the operation again.
```

```
ARA0002: Unable to restore FILE_SYSTEM asset F:\ because of an agent issue.

The restore was unsuccessful because of an agent issue.

The File System restore was unsuccessful because a Status code 500 error occurred during
the request to the Agent host.
```

Perform the operation again.

File sparseness and Linux file-level restores

Linux file-level restores of file-level backups do not retain file sparseness.

Use the appropriate tools to reduce disk space.

Restores of clustered drives fail with an agent host timed out error or a network connectivity error

When attempting to restore a clustered drive, you might see an error similar to one of the following:

```
The File System restore was unsuccessful because the request to the Agent host timed out.
```

```
ARA0005: Unable to restore FILE_SYSTEM asset C:\ClusterStorage\Volume3 because of a
network connectivity issue on agent host w2019c2.agent.com.

The restore was unsuccessful because of an issue with the network connection.

To resolve this issue: 1.Check the network connectivity between PowerProtect Data
Manager and the agent host. 2.Confirm that there is no packet loss between PowerProtect
Data Manager and the agent host.
```

Perform a full discovery of the logical cluster host, and then retry the restore. For more information about performing a full discovery, see the *PowerProtect Data Manager Administration and User Guide*.

Restoring block-based backups on 16 TB ReFS volumes

Image-level restore operations of File System agent block-based backups (BBB) might fail ReFS volumes with 16 TB or higher capacity.

Restore the data by using file-level restore (FLR).

Restoring multiple backups or SSIDs from the command-line interface

A single-level restore command-line interface (CLI) cannot be used to select multiple backups or SSIDs for restore.

Open a separate file-level restore CLI for each backup or SSID.

XFS restores of block-based backups

When performing an XFS restore of a block-based backup on a remote host, the kernel version of the remote host must be equal to or higher than the kernel version of the source host.

There is no workaround.

Storage units

You might encounter the following issues with storage units.

Creating storage unit fails when maximum MTree and Users count on DD system reached

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.

Discrepancy between storage unit capacity reported in PowerProtect Data Manager and DD Virtual Edition

Due to differences in space calculation (physical capacity vs. logical capacity), there is a discrepancy between storage unit capacity reported in PowerProtect Data Manager and DD Virtual Edition. For example, the DD storage unit capacity displayed in the **Protection** > **Storage** > **Manage Storage** window of the PowerProtect Data Manager UI might be greater than the amount displayed in DDVE.

To determine storage unit capacity, use DDVE instead.

B

– Glossary of Acronyms –

This glossary provides definitions of acronyms used in the PowerProtect Data Manager documentation.

Glossary

A

AAG: Always On availability group

ACL: access control list

AD: Active Directory

AKS: Azure Kubernetes Service

API: application programming interface

ARM: Azure Resource Manager

AVS: Azure VMware Solution

AWS: Amazon Web Services

AZ: availability zone

B

BBB: block-based backup

C

CA: certificate authority

CBT: Changed Block Tracking

CDC: change data capture

CIFS: Common Internet File System

CLI: command-line interface

CLR: Common Language Runtime

CN: common name

CPU: central processing unit

CR: custom resource

CRD: custom resource definition

CSI: container storage interface

CSV: Cluster Shared Volume

D

DA: database administrator

DAG: database availability group

DBID: database identifier

DDMC: DD Management Center

DDOS: DD Operating System

DDVE: DD Virtual Edition

DFC: DD Boost over Fibre Channel

DNS: Domain Name System

DPC: Data Protection Central

DR: disaster recovery

DRS: Distributed Resource Scheduler

DSA: Dell security advisory

E

EBS: Elastic Block Store

EC2: Elastic Compute Cloud

eCDM: Enterprise Copy Data Management

ECS: Elastic Cloud Storage

EFI: Extensible Firmware Interface

EKS: Elastic Kubernetes Service

ENI: Elastic Network Interface

EULA: end-user license agreement

F

FC: Fibre Channel

FCD: first class disk

FCI: failover cluster instance

FETB: front-end protected capacity by terabyte

FLR: file-level restore

FQDN: fully qualified domain name

FTP: File Transfer Protocol

G

GB: gigabyte
At Dell, this is 2^{30} bytes.

Gb/s: gigabits per second
At Dell, this is 2^{30} bits per second.

GCP: Google Cloud Platform

GCVE: Google Cloud Virtual Edition

GID: group identifier

GLR: granular-level restore

GUI: graphical user interface

GUID: globally unique identifier

H

HA: High Availability

HANA: high-performance analytic appliance

HTML: Hypertext Markup Language

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure

I

IAM: identity and access management

IDE: Integrated Device Electronics

IP: Internet Protocol

IPv4: Internet Protocol version 4

IPv6: Internet Protocol version 6

K

KB: kilobyte
At Dell, this is 2^{10} bytes.

L

LAC: License Authorization Code

LAN: local area network

M

MB: megabyte
At Dell, this is 2^{20} bytes.

ms: millisecond

MTU: maximum transmission unit

N

NAS: network-attached storage

NBD: network block device

NBDSSL: network block device over SSL

NDMP: Network Data Management Protocol

NFC: Network File Copy

NFS: Network File System

NIC: network interface card

NTFS: New Technology File System

NTP: Network Time Protocol

O

OS: operating system

OSS: open-source software

OVA: Open Virtualization Appliance

P

PCS: Protection Copy Set

PDF: Portable Document Format

PEM: Privacy-enhanced Electronic Mail

PIN: personal identification number

PIT: point in time

PKCS: Public Key Cryptography Standards

PSC: Platform Service Controller

PVC (cloud computing): private virtual cloud

PVC (Kubernetes): Persistent Volume Claim

R

RAC: Real Application Clusters

RAM: random-access memory

RBAC: role-based access control

ReFS: Resilient File System

REST API: representational-state transfer API

RHEL: RedHat Enterprise Linux

RMAN: `Recovery Manager`

RPO: `recovery-point objective`

RSA: `Rivest-Shamir-Adleman`

S

S3: `Simple Storage Services`

SaaS: `software as a service`

SAP: `System Analysis Program Development`
From the SAP website (2022), "the name is an initialism of the company's original German name: Systemanalyse Programmentwicklung, which translates to System Analysis Program Development. Today the company's legal corporate name is SAP SE - SE stands for societas Europaea, a public company registered in accordance with the European Union corporate law.

SCSI: `Small Computer System Interface`

SDDC: `software-defined data center`

SELinux: `Security-Enhanced Linux`

SFTP: `Secure File Transfer Protocol`

SLA: `service-level agreement`

SLES: `SuSE Linux Enterprise Server`

SLO: `service-level objective`

SPBM: `Storage Policy Based Management`

SQL: `Structured Query Language`

SRS: `Secure Remote Services`

SSD: solid-state drive

SSH: `Secure Shell`

SSL: `Secure Sockets Layer`

SSMS: `SQL Server Management Studio`

SSVs: `System Stable Values`

T

TB: `terabyte`
At Dell, this is 2^{40} bytes.

TCP: `Transmission Control Protocol`

TDE: `Transparent Data Encryption`

TLS: `Transport Layer Security`

TPM: `Trusted Platform Module`

TSDM: `Transparent Snapshot Data Mover`

T-SQL: `Transact-SQL`

U

UAC: user account control

UDP: User Datagram Protocol

UI: user interface

UID: user identifier

UTC: Coordinated Universal Time
From Wikipedia (2022), "this abbreviation comes as a result of the International Telecommunication Union and the International Astronomical Union wanting to use the same abbreviation in all languages. English speakers originally proposed CUT (for 'coordinated universal time'), while French speakers proposed TUC (for 'temps universel coordonné')."

V

VADP: VMware vStorage APIs for Storage Awareness

VBS: virtualization-based security

VCF: VMware Cloud Foundation

vCLS: vSphere Cluster Service

vCSA: vCenter Server Appliance

VCSA: vCenter Server Appliance

VDI: Virtual Device Interface

vDisk: virtual disk

vDS: virtual distributed switch

vFRC: Virtual Flash Read Cache

VGT: Virtual Guest Tagging

VIB: vSphere Installation Bundle

VLAN: virtual LAN

VM: virtual machine

VMC: VMware Cloud

VMDK: virtual machine disk

VNet: virtual network

VPC: virtual private cloud

vRSLCM: vRealize Suite Lifecycle Manager

VST: Virtual Switch Tagging

vTPM: Virtual Trusted Platform Module

VVD: VMware Validated Design

vVol: virtual volume

W

WAN: wide area network