

Technical White Paper

Dell PowerProtect Data Manager: File System Backup and Recovery

Abstract

This white paper focuses on file system backup and recovery using Dell PowerProtect Data Manager.

October 2022

Revisions

Date	Description							
July 2019	Initial release							
September 2019	Document revised for PowerProtect Data Manager version 19.2 release							
December 2019	Document revised for PowerProtect Data Manager version 19.3 release							
February 2021	Document revised for PowerProtect Data Manager version 19.7 release							
May 2021	Document revised for PowerProtect Data Manager version 19.8 release							
October 2021	Document revised for PowerProtect Data Manager version 19.9 release							
May 2022	Document revised for PowerProtect Data Manager version 19.10 release							
October 2022	Document revised for PowerProtect Data Manager version 19.12 release							

Acknowledgments

Author: Vinod Kumar Kumaresan

The information in this publication is provided "as is." Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

This document may contain certain words that are not consistent with Dell's current language guidelines. Dell plans to update the document over subsequent future releases to revise these words accordingly.

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

Copyright © 2022 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. [10/27/2022] [Technical White Paper] [H18659.7]

Table of contents

Rev	/ision	S	2
Ack	nowle	edgments	2
Tab	ole of	contents	3
Exe	cutive	e summary	4
Auc	dience	e	4
1	Intro	duction to Data Manager for File System	5
	1.1	Data Manager key features for file system protection and recovery	5
2	File S	System backup technology and models in Data Manager	6
	2.1	Block-based backup technology	6
	2.2	File-based backup technology	7
	2.3	Data Manager models for file system protection and recovery	7
	2.4	Roadmap to protect a file system	9
3	File S	System backup configurations	10
	3.1	File System Agent	10
	3.2	Enabling File System asset source	11
	3.3	File System host configuration	11
	3.4	File system asset discovery	12
	3.5	Protecting Windows clustered disks with Data Manager	13
4	File s	system protection policy	15
	4.1	Protection rule for file system	16
	4.2	Exclusion filters for file system data protection	16
	4.3	File system parallel backup settings	17
5	Data	Manager File System Backup	
	5.1	Centralized file system backup workflow	18
	5.2	Self-service file system backup workflow	19
6	Data	Manager File System Restore	20
	6.1	Centralized file system restore workflow	20
	6.2	Self-service file system restore workflow	21
	6.3	Centralized file-level restore of file systems	22
	6.4	Search support for file system workloads	22
	6.5	Self-service file-level restore of file systems	24
Α	Tech	nnical support and resources	25
	A.1	Related resources	25

Executive summary

Business Case: Challenges

Today's data protection is either too complex, requires multiple vendors, does not scale, or does not meet the needs of fast-growing, modern, and agile organizations of all sizes. As businesses continue to consume IT resources differently, there is a need for powerful, efficient, and trusted data protection to enable organizations to transform to meet future demands when modernizing their IT environment. One of the biggest challenges is determining how we can turn the data we protect and manage into value. Customers are challenged with backups, recovery, and ultimately the management and governance of the data they are protecting.

Solution Overview: Why PowerProtect Data Manager?

Dell PowerProtect Data Manager is the next generation data management platform to transform traditional data protection to comprehensive data management. Data Manager gives IT the trusted data protection they know from Dell Technologies, combined with operational simplicity that protects workloads and file systems running on-premises with self-service capabilities for operational efficiency and IT governance controls to ensure compliance. SaaS-based management makes it easy to monitor, analyze, and troubleshoot distributed data protection environments from anywhere.



Data Manager gives valuable insight into protected on-premises and in-cloud workloads, applications, file systems, and virtual machines. Designed with operational simplicity and agility in mind, Data Manager enables the protection of traditional workloads including Oracle, Exchange, SQL, SAP HANA, NAS, file systems, Kubernetes containers, and virtual environments.

This white paper focuses on file system backup and recovery with Data Manager, which ensures reliable and efficient data protection functionality. It also describes the file system backup architecture, backup and recovery workflows, and deployment requirements.

Audience

This white paper is intended for Dell Technologies customers, partners, and employees who are looking for file system data protection and management using Data Manager.

1 Introduction to Data Manager for File System

Data Manager offers centralized oversight of all protected file system copies. This makes it simple to track and enforce service level objective (SLO) compliance for backup and recovery, RPOs, and Storage retention lock. Data Manager discovers copies sent to protection storage, then catalogs and makes protection copies available for compliance measurement to ensure protection compliance and quality of service.

The File System Agent allows an application administrator to protect and recover data on the file system host. Data Manager integrates with the File System Agent to check and monitor backup compliance against protection policies. Data Manager File System Agent has been designed to support the file system backup, restore, and replication workflows. This white paper describes how effectively you can protect file systems using Data Manager with Dell PowerProtect DD series appliances as target storage.

1.1 Data Manager key features for file system protection and recovery

- Centralized file system backup and recovery (volume and file level) through Data Manager
- Self-service file system backup and file-level recovery (volume and file level) using command-line utility
- Block-based and File-based file system support for file system workloads. For more details on file system workloads compatibility, see section "File Systems" in the <u>PowerProtect Data Manager</u> <u>support matrix</u>
- Supports centralized file level restores of block-based file system backups.
- File level restore from Data Manager UI
 - Support restore to original or alternate host for file-based backups
 - o Creation of separate directory to separate the restore files
- Support for backup of Non-LVM or physical disks
- Supports exclusion of files and folders from file system backups through use of file exclusion
- Data Manager provides support to run file system backups in parallel to reduce the time taken for backups
- No excessive metadata generation and PowerProtect DD series appliances Active Tier storage consumption has been optimized for file-based backups
- Automated host agent configuration during policy creation
- Flexibility to define and assign exclusion filter to file system protection policy for excluding certain files and folders
- Encryption over the wire (EOW) of file system backup and restore data Data Manager provides EOW of data during some backup and restore operations. If enabled, encryption is automatically applied to file system workloads
- Data Manager File System Agent supports the Microsoft System State Recovery (SSR), Active Directory Restore, and bare-metal recovery (BMR) disaster-recovery mechanisms
- Data Manager File System agent now allows the selection of clustered drives and logical cluster hosts as assets and asset sources
- Starting with PowerProtect Data Manager 19.12, file indexing and search is supported for file system workloads

2 File System backup technology and models in Data Manager

2.1 Block-based backup technology

Data Manager performs a file system level full and incremental backup using block-based backup (BBB) technology. During the backup, the application agent scans a volume or a disk in a file system and backs up all the blocks that are in use in the file system. Unlike the traditional file system backup, BBB supports high-performance backups with a predictable backup window.



Figure 1: Data Manager Block-Based Backup Technology:

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 backup 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 series appliances
- DD retention lock
- Recoveries from DD series appliances

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%.

2.2 File-based backup technology

File-based backups (FBB) traverse through the entire directory structure of the file system to backup all the files in each directory of the file system. FBBs can provide additional capabilities such as exclusion. These backups take longer to complete when compared to block-based backups. The File System Agent performs a FBB of the protected assets when an exclusion filter is applied to a protection policy.

Note: Exclusion filters cannot be applied to self-service protection policies and to backups taken through self-service CLI.



Figure 2: Data Manager File-Based Backup Technology

2.3 Data Manager models for file system protection and recovery

File system protection data zone components include Data Manager server, PowerProtect File System Agents, file server host, and storage. Data Manager for file system protection has been built with two service model features:

- a) Self-service file system protection and recovery
- b) Centralized file system protection and recovery



Figure 3: Data Manager models for file system protection and recovery

a) Self-service file system protection and recovery

- File system admin or user can use self-service CLI commands to perform self-service backup or restore
- For a host with File System Agent installed, a Data Manager server is required to backup file systems. However, a backup administrator or file system administrator who wants to back up file systems manually (and who uses Data Manager only for compliance purposes) can register the host to Data Manager and create a self-service protection policy to configure only the retention policy instead of a complete backup schedule.
- After a host is registered with Data Manager and assets are added to a self-service protection policy, selfservice or manual backups can be performed on the host's file system assets by using the (ddfssv) command-line utility.
- Self-service restore can restore from backups that were centralized or self-service and can be done to a local or remote server.

Note: To enable self-service protection, self-service protection option is selected when creating the file system protection policy in the Data Manager.

b) Centralized file system protection and recovery

- Centralized file system model is built for backup administrators to perform policy-based file system backup, recovery, replication, and long-term retention of copies. With the centralized protection feature, Data Manager manages the entire file system backup workflow, including the schedule.
- Centralized protection is supported through protection policy. After the File System Agent is installed on the client, the client is auto discovered on Data Manager and enables the administrator to approve the client.
- Choosing the centralized protection option during protection policy creation enables Data Manager to manage all protection centrally.

2.4 Roadmap to protect a file system

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



Figure 4: Roadmap to protect a file system

See <u>PowerProtect Data Manager File System Agent User Guide</u> for details about how to install, configure, and perform a file system backup/restore.

3 File System backup configurations

3.1 File System Agent

The File System Agent needs to be installed on the host that is planned to protect. The File System Agent binaries (Windows and Linux) can be downloaded on the below path from **PowerProtect Data Manager** \rightarrow **Settings** \rightarrow **Agent downloads**.

Downloads			
Agent WinPE Kubernetes VMware	File System File System Agent for Linux or Windows or AIX Version 19.12-21 Download Agent ▼ Download for Windows Download for Linux	Cracle Cracle Oracle RMAN Agent for Linux or AIX Version 19.12-21	SMIS Server Allows protection of storage arrays Version 19.12-21 Download Agent ◄
	Download for AIX Agent for Microsoft Exchange Server Version 19.12-21 Download Agent	Signature Microsoft SQL Server Agent for Microsoft SQL Server on Windows Version 19.12-21 Download Agent	SAP HANA Linux agent for SAP HANA Version 19.12-21 Download Agent

See <u>PowerProtect Data Manager File System Agent User Guide</u> for details on how to install File System Agent on supported Windows and Linux hosts.

Data Manager supports the coexistence of agents on the same Windows or Linux host for the following:

- Microsoft SQL agent and the File System Agent on Windows
- Microsoft Exchange agent and the File System Agent on Windows
- Oracle RMAN agent and the File System Agent on Linux
- SAP HANA agent and the File System Agent on Linux

Software compatibility information for the Data Manager software and the File System Agent is provided in the eLab navigator, available at https://elabnavigator.dell.com/eln/modernHomeDataProtection.

3.2 Enabling File System asset source

By enabling the file system asset source, Data Manager can protect and recover file system data when Data Manager is integrated with the File System Agent.



3.3 File System host configuration

After the File System Agent is installed on the file system host, File System Agent can be added, approved, and rejected for the pending agent requests. Select **Infrastructure** > **Application Agents** and click **Add** or **Approve** as required.

The "Auto Allow List" all option is disabled by default. When enabled, all preapproved application agents are automatically approved.

Pov	verProtect Data Mar	ager	5						e	D Q D	@• @• ≗	• ==
(3 2 5)	Dashboard Health Infrastructure	~	Application Agent registration	Agents	aiting Approval	l.	O Approved		2 Registered	I	0 Rejected	
	Assets Asset Sources Storage Protection Engines Application Agents		Agent update st	atus: 🥏 2 dit Remove	Up to Date	O Availa Reject	ble Export All	© 0 Scheduled More Actio	o In Pro	ogress	C Failed	∨ ow List
	Search Engine Networks Protection	>	Details	Host Name windows1.tme.	ע וף local	♥ Regis	tration Status	Y I OS Y WINDOWS	Agent Type Y	Current Version	Update Stat	us 🍸
0 4 *	Restore Alerts Administration	>		windows.tme.lc	ical	Regis	tered	WINDOWS	File System Agent	19.12	O Up to	o date
С П	Reports Jobs	> >	4									

File System Agent registered with Data Manager:

On successful registration, the file system host is listed on the **Infrastructure** > **Asset Sources** section. Asset discovery is initiated by default after registration of the file system host to Data Manager.

File system host is discovered in the **Asset Sources > File System** section.

Pov	verProtect Data Man	ager								Ę	Q	۵		⊘∙	≗•	88
ŵ	Dashboard		Asset Sour	rces												
₹4 %	Health Infrastructure	~	vCenter	File System	•											
	Assets Asset Sources		Discover	Delete	How to a	dd File System Host	Q Search									
	Storage Protection Engines		Name	e		V4 Stat	us 🏾 🍸	Туре	Discovery St	atus		Last	Discovery	/		
	Application Agents		O wind	lows.tme.local		Ava	ilable	FS	OK			Oct 1	19, 2 022,	4:30:38 F	PM	
	Search Engine Networks		O wind	lows1.tme.local		Ava	ilable	FS	ОК			Oct 1	19, <mark>2</mark> 022,	4:50:13 F	PM	
1	Protection	>														
3	Restore	>														
Δ	Alerts															

3.4 File system asset discovery

Discovered file system assets in the **Infrastructure > Assets** section.

Pov	verProtect Data Ma	nager							Ę	Q	۵	¢¢،		8∙	88
(j 2)	Dashboard Health		Assets Virtual Machine File System												
8	Assets Asset Sources	×	Back Up Now View Copies	Export A	II More Actio	ns 🔻 🔍 🔍	Search							ŧ	=
	Storage Protection Engines		Name	Status	Protection P	OS Type	Size	File Syst	Last	Сору				Netwo	rk
	Application Agents Search Engine		✓	Available											
	Networks		C (Available	File System	WINDOWS	42.4 GB	NTFS	Oct 1	7, 2022, 1	0:46:57 /	M			
Ī	Protection	>	Disaster Recovery	Available	File System	WINDOWS	42.5 GB	FS_DR	Oct 1	7, 2022, 1	0:49:08 /	M			
C)	Restore	>	□ E\	Available	File System	WINDOWS	21.3 GB	NTFS	Oct 1	7, 2022, 1	0:46:58 /	M			
4	Alerts		E\	Available	File System	WINDOWS	21.3 GB	NTFS	Oct 1	7, 2022, 1	0:46:59 /	M			
щ	Administration Reports	>	windows1.tme.local	Available											
٢	Jobs	>	Show 50 v per page									~	1 of	1 >	>>

3.5 Protecting Windows clustered disks with Data Manager

Starting with Data Manager version 19.10, the File System Agent provides support for protecting the Windows clustered file system. With this feature, customers can use the File System Agent to protect their clustered disks, like the regular file system drives.

Both BBB and FBB are supported for Windows clustered disk protection. During the failover, the backup will continue through the node that owns the cluster disks. This prevents administrators from having to manually reconfigure for data protection continuity.

The following figure shows the **Application Agents** view for the Windows cluster nodes registered with Data Manager.

Pov	verProtect Data Man	ager								Q 🖉	©• ≗• © (D• 88
3 %	Dashboard	~	Application Agents									
	Assets Asset Sources		Agent registration status:	O Awaiting Approval			O Approved	I	2 Registered		O Rejected	
	Storage Protection Engines		Agent update status:	2 Up to Date	1	O Available	l,	0 Scheduled	🞯 0 In Progress	1	O Failed	~
	Application Agents Search Engine Networks		Add Approve	Reject Edit	Remove	More Actions 🔻	Q Search				Auto	Allow List
T	Protection	>	Details	Host Name	\ ⟨IP	\ F	legistration Sta	♡ OS	♥ Agent Type ♥	Current Version	Vpdate Status	V
S	Restore	>	o G	I1dpdmgt206.soltme.local		ş	Registered	WINDOWS	File System Agent	19.10	🕑 Up to date	
\$	Alerts Administration	>	o G	11dpdmgt205.soltme.local		F	Registered	WINDOWS	File System Agent	19.10	Up to date	
щ	Reports	>										
٢	Jobs	>										

The above cluster nodes registered with Data Manager discover the clustered disks as assets, as shown below.

Pov	verProtect Data Manag	jer						
ିର	Dashboard		Assets					
80	Infrastructure Assets	~	Virtual Machine File System					
	Asset Sources Storage Protection Engines		Back Up Now View Copies	More Actio	Q Search			
	Application Agents		Name	Status	Protection Policy	OS Type	Size	File System T
	Search Engine		▼ 🗌 🚦 I1dpdmgt205.soltme.local	Available				
	Networks		🗌 🖻 C:\	Available	FS_CSV_Backup	WINDOWS	53.1 GB	NTFS
I	Protection	>	Disaster Recovery	Available	FS_CSV_Backup	WINDOWS	53.2 GB	FS_DR
3	Restore	>	▼	Available				
Δ	Alerts		P= C:\	Available		WINDOWS	53.1 GB	NTFS
20	Administration	>	Disaster Recovery	Available		WINDOWS	53.2 GB	FS DR
щ	Reports	>	The Cluster 01					
٩	Jobs	>	C:\ClusterStorage\Volume2	Available	FS_CSV_Backup	WINDOWS	10.7 GB	CSVFS
				Available	FS_CSV_Backup	WINDOWS	21.3 GB	NTFS

A file system protection policy can be created to back up the cluster assets, in the same way of protecting the regular file system drives.

Po	werProtect Data Ma	inage	r					Q	2	©• ،	3 ► (1 ?∙
୍ଥ	Dashboard			Edit Policy								
80	Infrastructure	>										
1	Protection	~		Туре	Assets							
	Protection Policies SLA Compliance			Purpose	Edit the following asset selection for protection by this policy. Know more		Name: FS_CS	V_Backup Typ	e: File Syster	n Purpo	se: Cent	tralized Prote
	Protection Rules			Assets	Q Search							
S	Restore	>		File Exclusions	Name	Status	Protection Policy	Size	File	e System		Network
\triangle	Alerts			Objectives	E 🔄 📋 I1dpdmgt205.soltme.local	Available						
ം	Administration	>		Options	✓ Pi CA	Available	FS_CSV_Backup	53.1 GB	NT	FS		
ш	Reports	>			 Disaster Recovery 	Available	FS_CSV_Backup	53.2 GB	FS.	_DR		
٩	Jobs	>		Summary	I1dpdmgt206.soltme.local	Available						
					▼							
					C:\ClusterStorage\Volume2	Available	FS_CSV_Backup	10.7 GB	CS	VFS		
					🗹 🖻 E/	Available	FS_CSV_Backup	21.3 GB	NT	FS		

Backup copies available for Windows cluster assets.

Po	werProtect Data Ma	anage	er
Ś	Dashboard		Restore
80	Infrastructure	>	Vidual Mashing
T	Protection	>	Virtual Machine File System
S	Restore	~	View Copies Q Search
	Assets		
	Running Sessions		Name Status Protection Policy OS Type Size File System T
\bigtriangleup	Alerts		Ildpdmgt205.soltme.local Available
20	Administration	>	Cluster01
щ	Reports	>	C:\ClusterStorage\Volume2 Available FS_CSV_Backup WINDOWS 10.7 GB CSVFS
٩	Jobs	>	○ E E\ Available FS_CSV_Backup WINDOWS 21.3 GB NTFS

Once the backup is successful, Data Manager provides the option to perform FLR and Image level restore to the original, or to an alternate location, from the backup copy.

P	owerProtect Data Man	ager								Q	¢۵ ک	}•	≗• ©	
ଜ	Dashboard		← Restore » Asset C:\ClusterStore	age\Vo	olume2									
80	Infrastructure	>	Olisis on the inertial below to view the stressed terrate and											
1	Protection	>	Click on the icon(s) below to view the storage targets and copies.	00 110	dpdvcld089.hop.lab.emc.com									
S	Restore	~		Location	Not Assigned				Capacity: 326.3 GB Used: 27.6 GB					
	Assets Running Sessions			Res	tore To New Restore	To Origin	al File L	evel Restore						
\triangle	Alerts													
ಿಂ	Administration	>			Create Time	$\downarrow \forall$	Size	Retention		Copy Status	V	Lo	cation	V
щ	Reports	>			Mar 20, 2022, 12:47:06 AM		335.6 MB	Mar 22, 202	2, 5:30:00 AM	Available		L	ocal	
Θ	Jobs	>		0	Mar 20, 2022, 12:40:32 AM		335.6 MB	Mar 22, 202	2, 5:30:00 AM	Available		L	ocal	

4 File system protection policy

A file system protection policy can be created from Data Manager UI to protect file system data.

Protection life cycle policy defines a set of objectives that apply for a specific duration. Data Manager provides centralized and self-service protection options to specify one of the following "Purposes" for the protection policy to back up Linux/Windows file systems. These objectives drive configuration, active protection, and data management operations that satisfy Service Level Agreements (SLAs).

For file system protection, you can select one of three types:

Pov	verProtect Data Mar	ager			町 Q Q @• @• Z• H
G 2 & 🖱 🖓 🖓	Dashboard Health Infrastructure Protection Protection Policies SLA Compliance Protection Rules File Exclusion Restore Alerts	>	Add Policy Type Purpose Assets File Exclusions Objectives	~	Purpose Select the purpose for this policy. Name: File System Type: File System Over Protect Data Manager centrally manages all stages of the protection policy and also enables the self-service operations. Self-Service Protection Your backup application handles the local protection stage. PowerProtect Data Manager handles the additional stage by protecting selected assets within a protection policy. Exclusion
С. Щ %	Administration Reports Jobs	>	Summary		Select this option to assign specific assets to an exclusion policy of that these assets do not display as Unprotected. An exclusion policy prevents these assets from being assigned to any other protection policies. Asset assignment to an exclusion policy can occur manually or automatically, based on existing protection rules.
⊛					

- Centralized Protection To use Data Manager to manage all protection centrally.
- Self-Service Protection To use the file system to create local backup protection. Data Manager creates a protection policy and manages extra stages.
- Exclusion If there are assets within the protection policy to exclude from data protection operations.

Option to enable indexing for file search and restore from the protection policy, when one or more search nodes are deployed with PowerProtect Data Manager.

Pov	verProtect Data Ma	nager					Ę	Q	۵	۵.	⊘►	4℃	88
6) 12	Dashboard Health		Add Policy										×
‰	Infrastructure	>	Туре	~	Options								
7	Protection Protection Policies	~	Purpose	~	Select additional op	tions for this policy. Name: File System Type: File Syste	m Pur	pose: Cer	tralized	Protectio	n Assets	s: 4	
	SLA Compliance		Assets	~	Advanced options								
	Protection Rules File Exclusion		File Exclusions	~	Enable indexing for file search and restore	Enable indexing for file search and restore	Ð						
C	Restore	>	Objectives	~									
\bigtriangleup	Alerts		Options		Disaster recovery options	 Back up system state files only () Ignore missing system state files () 							
2¢	Administration	>	Summary			Exclude non-critical dynamic disks ()							
щ	Reports	>	Guinnary			Note: These options apply only to disaster reco	very ob	jects.					
•	Jobs	>			•								Þ

After the policy configuration is complete, an informational message appears to confirm that Data Manager has saved the protection policy. Initially there will be two configuration tasks running:

- > The first task will create a storage-unit on DD series appliance.
- The second task will update the agent lockbox on the file system host and add the new storage-unit credentials.

	Job ID 🛟 🏹	Status T	Description	Ĵ ♡ Job Type Ĵ ♡
0	OQKTYURH	Success	Configuring File System - Filesystem_Backup	Config
0	80VM2YS0	Success	Performing Policy Configuration - Filesystem_Backup - PROTECTIO	N Config

See <u>PowerProtect Data Manager File System Agent User Guide</u> for detailed steps on how to create a protection policy for file system backup.

4.1 Protection rule for file system

A protection rule automatically determines which assets get assigned to protection policies when the assets are discovered. A protection policy must exist prior to creating the dynamic filter. An asset can only belong to one protection policy.

Pov	werProtect Data Manager			Q Д ፟፟፟፟ ፟ ፟€• 0 ∅• ⊞
ය %	Dashboard	Add Protection Rule		×
	Assets Asset Sources Storage Protection Engines	Select Protection Policy	d Conditions ct conditions to assign assets to the policy	Policy Name : Filesystem_Backup Rule Name : Filesystem View Filtered Assets - 0
	Application Agents Search Engine Networks Protection Protection Policies SLA Compliance	Add Conditions Summary	File System Name Begins with Host Name Contains Host Type Does not contain	ă ×
N 4	Protection Rules File Exclusion Restore > Alerts		File System Type Does not equal File System Size Ends with Equals	
20	Administration Access Control Credentials Certificates Audit Logs		Matches RegEx Does Not Match RegEx 3 of 4	Cancel Back Next

4.2 Exclusion filters for file system data protection

Data Manager provides the option to exclude data (file system files and folders) from assets that are assigned to protection policies. File system exclusion filters can be defined and applied to a protection policy to exclude certain files and folders from file system data protection.

An exclusion filter provides the following options for excluding file and folders from a file system backup.

PowerProtect Data Manager		
Add Filter		×
Filters	Filter Information Name · FSBackup	
	Description	
	+ File Size + File Type + Modified Time + Folder Path × File Size: Less than or Equal to ▼ 10 GB ▼ and × File Type: Less than or Equal to ▼ 10 GB ▼ and	
	× Folder Path: /tmp and × Modified Time: After • 08/09/2021 11:50 AM Image: Content of the second	
	The use of exclusion filters on PowerProtect Data Manager cloud deployments might result in heavy consumption of metadata. Exclusion Filters No exclusion filters et.	Add Filters
	Step 1 of 2	Cancel Next

Exclusion Filter Conditions								
Conditions	Description							
File Type	For exampletxt, .xlsx, .pdf							
Modified Time	File/Folder modification time							
File Size	File/Folder size							
Folder Path	File/Folder path							

After the filters are created, filters can be applied during the new file system protection policy creation or it can be applied to an existing file system protection policy. For verification, backup logs provide details of the files and folders which are excluded from backup according to the filter defined.

4.3 File system parallel backup settings

Data Manager enables running file system backups in parallel to reduce the time taken for backups. This setting defines the maximum concurrent network sessions from the client to DD series appliance at any given time. The number of streams to use for the backup can be specified in the configuration file ..ddfssv.fsagentconfig or through the self-service CLI. However, it is best to set the parallelism value in the configuration file because 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. Because the parallelism setting is defined at the host level, the parallelism setting must be set on every Windows host where parallel file system backups are enabled. This value must be an integer. The default value is 8.

See <u>PowerProtect Data Manager File System Agent User Guide</u> for details on how to specify the number of streams to use for the backup in the .ddfssv.fsagentconfig file in the C:\Program Files\DPSAPPS\fsagent\settings directory on the file system host or by using the command-line option.

5 Data Manager File System Backup

Data Manager enables discovering, managing, monitoring data protection, and replicating file system assets through integration with the File System Agent. File system assets are protected in Data Manager with centralized and self-service file system protection features.

Data Manager self-service protection enables users to perform backup and restore using a self-service CLI workflow for Windows and Linux assets. With agility and self-service feature, data owners can perform backup and recovery within native applications.

5.1 Centralized file system backup workflow



Figure 5: Centralized file system backup workflow

- 1. Protection policy is created for centralized File System protection.
- 2. At the time of scheduled backup, the Data Manager requests the File System Agent to perform save operation for the file system data.
- 3. File System Agent parses the backup job request and converts into (ddfssv) utility commands to perform save operation.
- File System Agent verifies DD series appliance connectivity and writes the file system data to the storageunit created on the DD series appliance. (Waits for 15 minutes)
- 5. File System Agent writes the catalog details to catalog database on Data Manager.
- 6. ADM agent retrieves the result from FS agent and updates the backup status to Data Manager.
- 7. Creates and maintains Protection Copy Set (PCS) in Elasticsearch database

5.2 Self-service file system backup workflow

A host with the File System Agent installed requires Data Manager to back up the file systems. To back up file systems manually and use Data Manager, the file system host needs to be registered with Data Manager and a self-service protection policy needs to be created. Data Manager discovers these backups and enables centralized restore operations. You can also perform a manual restore operation.



Figure 6: Self-service file system backup workflow

- 1. Protection policy is created for self-service File System protection.
- File system administrator launches the (ddfssv) utility using command line on the file system host and inputs the below details to initiate backup. Backup schedule (Full, Incremental) Storage IP address Storage Username Storage password
- 3. (ddfssv) utility performs save operation.
- File System Agent verifies DD series appliance connectivity and writes the file system data to the storageunit created on the DD series appliance. (Waits for 15 minutes)
- 5. File System Agent writes the catalog details to catalog database on Data Manager.
- 6. ADM agent retrieves the result from FS agent and updates the backup status to Data Manager.
- 7. Creates and maintains Protection Copy Set (PCS) in Elasticsearch database

6 Data Manager File System Restore

When file systems are protected within a protection policy in a Data Manager, the file system data can be recovered using the centralized restore functionality or by directly using the self-service restore feature.

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 enough space available on the target volume for the restore

6.1 Centralized file system restore workflow

A file system host image-level restore allows recovering data from backups of file systems performed in Data Manager.



Figure 7: Centralized file system restore workflow

- 1. Backup administrator creates the recovery job on Data Manager UI with below UI inputs,
 - Source file system backup
 - Destination file system
 - Restore options
 - Restore file location
- 2. Data Manager requests its ADM agent to dispatch the restore operation to File System Agent.
- 3. File System Agent parses the recovery job request and converts into (ddfsrc) utility commands and executes the restore operation based on inputs provided.
- 4. File System Agent verifies DD series appliance connectivity and the requested file system data is restored to the specified destination.
- 5. ADM agent retrieves the result from File System Agent and updates the restore status to Data Manager.

Note: If the destination file system asset already contains some data, this data will be overwritten.

6.2 Self-service file system restore workflow

Self-service image-level restores of file systems can be performed 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

Before running the (ddfsrc) command to perform a self-service image-level restore of file Systems, the (ddfsadmin) backup command can be used to query a list of all the local backups taken for a host and obtain the ID of the save set for restore, Specify the ID of the save set as an input to the ddfsrc command. If restoring to the original host, the password will be picked up from the lockbox.



Figure 8: Self-service file system restore workflow

- File system administrator launches the ddfsrc command-line utility and below details to be entered as input, Once the inputs are validated and executed the ddfsrc utility performs recover operation. Source file system backup Destination file system Restore options Restore file Location
- 2. File System Agent verifies DD series appliance connectivity and the requested file system data is restored to the specified destination.

The self-service restore feature provides the following options to restore the data:

- Restore to same host and same location
- Restore to same host and different location
- Restore to different host and location

6.3 Centralized file-level restore of file systems

Data Manager provides the option to restore files and folders from file system backup through Data Manager centralized console.

Recovery > Assets > File Level Restore

Pov	verProtect Data Man	ager						Q	4	€.	₽►	í	?►	88
ŝ	Dashboard		← Restore » Asset C:\											
80	Infrastructure	>	Click on the icon(s) helow to view the											
9	Protection	~	storage targets and copies.	dd dd	ve.hop.lab.emc.	com			004 0 00					
	Protection Policies			Location:	Not Assigned			Used: 14.	326.3 GB) GB					
	SLA Compliance		FS DD							_				*
	Protection Rules			Res	tore To New	Restor	e To Original	File Level	Restore	•				- 1
	File Exclusion													
S	Restore	~			Create Time	$\checkmark \forall$	Size	Retention	*	Copy .	. • 7	Loc	ati 🗘 🦷	7
	Assets		•		Aug 20, 2021 (1.16.96 DM								
	Running Sessions				Aug 29, 2021,	11:10:30 PIVI	12.2 GB	Sep 1, 2021, 5:30:0	MA 0	Availa	ble	Lo	cal	
\bigtriangleup	Alerts													
ç	Administration	>												
\odot	Jobs	>												
а	Reporting													
	Reporting													
Ð														

File and folder level restore can be done to the same or alternate host, where the alternate host needs to be registered with Data Manager.

Select Target Host and Mount										
 Restore to same/original machine l1dpdmgt174 Restore to alternate host 										
Mount										

6.4 Search support for file system workloads

Starting with PowerProtect Data Manager 19.12, file indexing and search is supported for file system workloads. As a prerequisite, one or more search nodes must be deployed. Indexing for file search and the restore option is enabled from the protection policy.

When the file system backup is completed, the **File Search** option is available to search and restore the required files.

Pov	verProtect Data Mar	nager							Ę (ς Δ		⊘►	٩₽	88
ŝ	Dashboard		Restore											
	Health													
80	Infrastructure	>	Virtual Machine	ile System										
Ī	Protection	>	View Copies	File Search E	Export All	Q Search							1	
\square	Restore	~												
	Assets		Name	Status	Protection .	OS Type	Size	File Sy	Last	Сору			Netv	vork
0	Running Sessions		✓ windows.tme.local	Available										
25	Administration		⊖ c:\	Available	File System	WINDOWS	42.4 GB	NTFS	Oct 1	7, 2022, 10:	46:57 AM			
¢2 بيا	Reports	Ś	Disaster Recovery	Available	File System	WINDOWS	42.5 GB	FS_DR	Oct 1	7. 2022. 10:	49:08 AM			
<u> </u>	lobs	Ś		Available	Eilo Suotom	WINDOWS	21.2 CP	NITES	Oct 1	7 2022 10-	46·50 AM			
1	0000	-		Available	File System	WINDOWS	21.5 66	NIFS	OCL	r, 2022, 10.	40.36 AIVI			
			○ F:\	Available	File System	WINDOWS	21.3 GB	NTFS	Oct 1	7, 2022, 10:	46:59 AM			
			Show 50								• Rêr bi	age 1 of	1 >	>>

The **"FS File Search**" window provides the ability to search for the required files using the different search criteria options.

PowerProtect Data Manager				Ę Q	众 ‡• ?• ≗• ⊞						
Dashboard Restore > FS File Search											
Health Search Criteria	Clear All File/Folder Name: dsta01 ×										
File Name data01	 Results (5) 	 Results (5) 									
C Restore V File Type	Details Name	↑ Folder Path	File System Name	Host Address	Backup Date						
Assets .txt	● 🔂 Data01.txt	/Backup05/	E:\	windows.tme.local	Oct 17, 2022, 10:46:58 AM						
Alerts	O 🕻 Data01.txt	/Backup03/	E:\	windows.tme.local	Oct 17, 2022, 10:46:58 AM						
& Administration > Folder Path	O 🔂 Data01.bxt	/Backup02/	E:\	windows.tme.local	Oct 17, 2022, 10:46:58 AM						
<u>∎l</u> Reports > Enter Folder Path	O 🔂 Data01.txt	/Backup01/	E:\	windows.tme.local	Oct 17, 2022, 10:46:58 AM						
Jobs Show Only Files : Off	O 🔓 Data01.bit	/Backup04/	E:\	windows.tme.local	Oct 17, 2022, 10:46:58 AM						
File System Name											
E\ 🗸											
Host Address											
Enter Host Address											
Last Backup Only : Off	4				Þ						
Backup Date	1 - 5 of 5 items Show: 25 🗸 per	rpage									
Date Modified	1 item selected (Ready to add)										

File search and restore options:

- Restore to original host Select this option to restore files and/or folders to the original host.
- Restore to alternate host Select this option to restore files and/or folders to an alternate host.

Pov	verProtect Data Ma	nager								Þ	Q	Ą	•	?∙	4℃	
습 문	Dashboard Health		File System Restore													×
80	Infrastructure	>	File Search 🗸	L	ocatio	n										
1	Protection	>	Location		 Restore to original host 											
ດ 4	Restore Assets Running Sessions Alerts	×	Summary	(Select this option to restore files and/or folders to the original host. Restore to alternate host Select this option to restore files and/or folders to an alternate host.									te:		
°°	Administration	>														1
Щ Ш	Reports	>				Name 🛛 🍸	Status 🍸	Host/Cluster/Group Name	OS Type		Size		File Sys	tem Type	Y	
9	Jobs	>			0	Disaster Recovery	Available	windows1.tme.local	WINDOWS		42.5 GB		FS_DR			
					\bigcirc	C:\	Available	windows1.tme.local	WINDOWS		42.4 GB		NTFS			
					\bigcirc	ΕX	Available	windows1.tme.local	WINDOWS		21.5 GB		NTFS			
					\bigcirc	H:\	Available	windows1.tme.local	WINDOWS		21.5 GB		NTFS			
					0	G:\	Available	windows1.tme.local	WINDOWS		21.3 GB		NTFS			
					0	F:\	Available	windows1.tme.local	WINDOWS		21.3 GB		NTFS			
e					0	E:\	Available	windows1.tme.local	WINDOWS		21.3 GB	1	NTFS			

6.5 Self-service file-level restore of file systems

Self-service file-level restores of file systems can be performed using the ddfsrc command with the -I option. A file that contains the list of file(s) to be restored is created before executing the command. The location of this file is given as an input to the -I option.

For more details on performing self-service file-level restore of file systems, see <u>PowerProtect Data Manager</u> <u>File System Agent User Guide</u>.

A Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

The <u>Data Protection Info Hub</u> provides expertise that helps to ensure customer success with Dell data protection products.

A.1 Related resources

- <u>PowerProtect Data Manager File System User Guide</u>
- PowerProtect Data Manager Administration and User Guide
- PowerProtect Data Manager Deployment Guide
- PowerProtect Data Manager Compatibility Matrix