PowerProtect Data Manager: VMware Virtual Machine Protection Using Transparent Snapshots

March 2026

H18884.12

White Paper

Abstract

This white paper provides insights into how to protect and restore VMware virtual machines using transparent snapshots available with Dell PowerProtect Data Manager.

DELL Technologies

Copyright

Contents

Executive summary

Overview

This white paper describes how to protect and restore VMware virtual machines using transparent snapshots available with Dell PowerProtect Data Manager. It details the architecture and life cycle of transparent snapshots and describes how this capability is integrated with PowerProtect Data Manager. It also includes an overview of the process for restoring virtual machines and presents test results that show the performance benefits of this solution.

Revisions

Date	Part number/ revision	Description
September 2021	H18884.1	Initial release
December 2021	H18884.2	Content updates
March 2022	H18884.3	Update for PowerProtect Data Manager 19.10
October 2022	H18884.4	Update for PowerProtect Data Manager 19.11 and 19.12
March 2023	H18884.5	Minor updates
June 2023	H18884.6	Updated to include PowerProtect Data Manager 19.13 enhancements
July 2023	H18884.7	Updated to include PowerProtect Data Manager 19.14 enhancements
December 2023	H18884.8	Update for PowerProtect Data Manager 19.15
March 2024	H18884.9	Update for PowerProtect Data Manager 19.16
July 2024	H18884.10	PowerProtect Data Manager 19.17 updates and general additions
November 2024	H18884.11	PowerProtect Data Manager 19.18 updates and general additions
March 2026	H18884.12	Recent Transparent Snapshots enhancements in PowerProtect Data Manager

We value your feedback

Dell Technologies and the authors of this document welcome your feedback on this document. Contact the Dell Technologies team by email.

Author: Idan Kentor

Note: For links to other documentation for this topic, see the PowerProtect Data Manager Info Hub.

Introduction

The VMware virtual machine (VM) backup process transfers or exports data from a VM within a VMware environment to a secondary protection storage system. The Dell PowerProtect appliance can be on a primary or secondary site, or in the cloud. A backup engine or software such as PowerProtect Data Manager manages this process. PowerProtect Data Manager can perform data management and copy management operations on the backup copies and ensure that all data is cataloged properly. This function makes available a consistent VM copy as part of a restore requirement in a disaster scenario.

PowerProtect Data Manager can protect VMware VMs in a reliable and efficient manner using VMware vSphere Storage APIs - Data Protection (VADP) snapshots (see Figure 1). These VADP snapshots are reliable, proven, and certified by VMware, and can be used as part of backup operations.

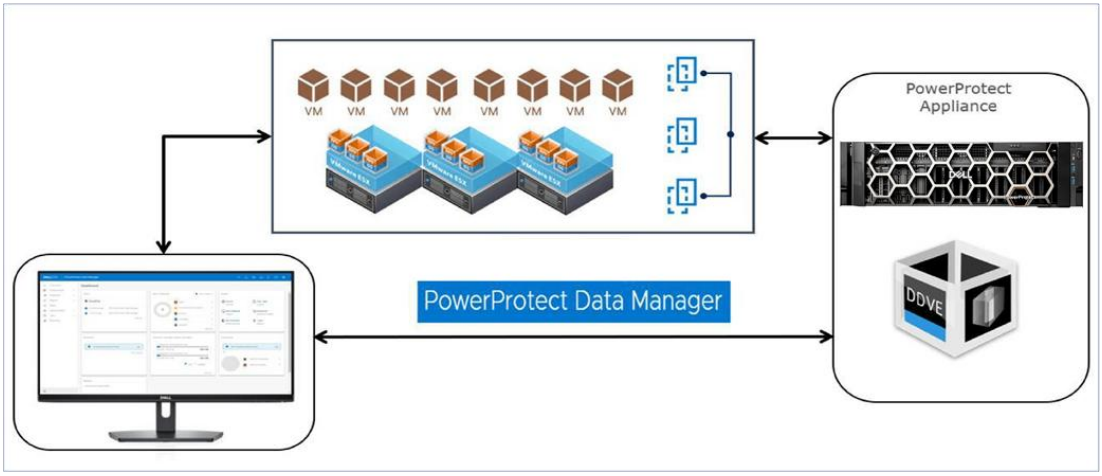


Figure 1. PowerProtect Data Manager for VMware

However, the VADP snapshot process pauses the execution of the VM and allows in-flight disk I/O operations to be completed. This action might increase the read and write latency and affect the snapshot and VM ecosystem life cycle. When the life cycle of a VADP snapshot is analyzed, the snapshot entry and exit points inflict a penalty on a VM. After a snapshot of a VM disk file is produced, requiring the VM to be stunned, a snapshot of the VM disk file is ingested. Then, the deltas must be consolidated into the base disk. When you create a snapshot of a high-transactional application, such as a database, there can be adverse effects. These effects include lengthy backup windows and application timeouts when the stun to ingest and consolidate the workflow is not efficiently managed.

Addressing these issues requires a solution that can deliver not only backup and restore capabilities but also an alternative way to reduce the adverse effects of the VM stun operation.

Transparent snapshots architecture

As shown in Figure 2, PowerProtect Data Manager transparent snapshots use the vSphere API for I/O (VAIO) Filtering framework. The transparent snapshots data mover (TSDM) is deployed in the VMware ESXi infrastructure through a PowerProtect Data

Manager VIB. This deployment creates consistent VM backup copies and writes the copies to the protection storage (PowerProtect appliance).

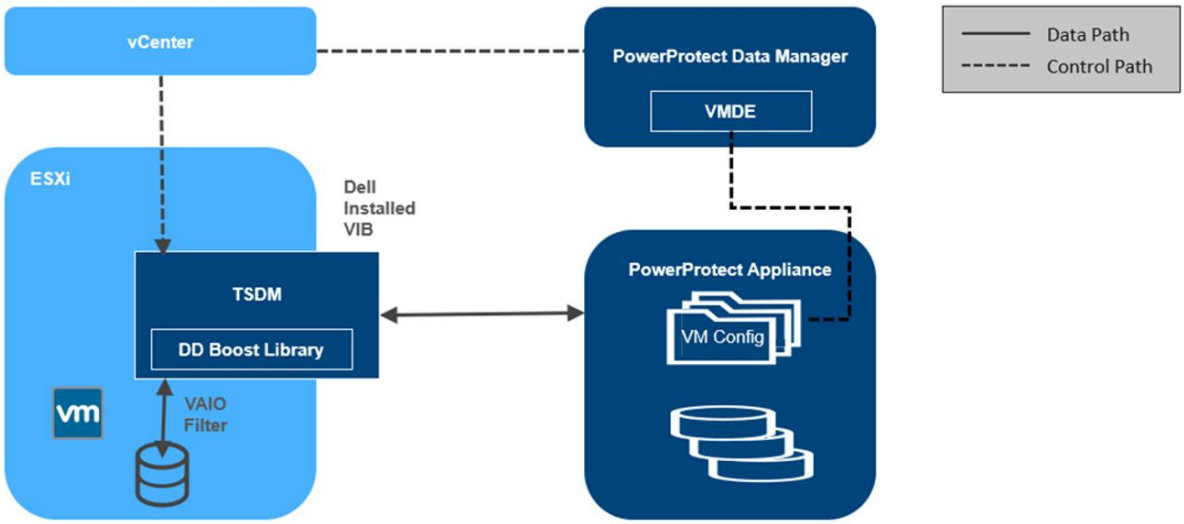


Figure 2. Transparent snapshots architecture

On the control and data paths:

- PowerProtect Data Manager assumes the role of an orchestrator where it identifies the VM assets in the VMware environment and provides scheduling capabilities.
- PowerProtect Data Manager uses VM Direct Engine (VMDE) to communicate with the VMware vCenter level APIs provided by VMware. The VM Direct Engine communicates with vCenter to achieve the following two key tasks:
  - Creates and tracks the progress of the vCenter level tasks that are visible to the end users, such as sync, restore, and snapshot operations.
  - Is responsible for locating the relevant ESXi host on which the operation (backup or restore) is to be performed, based on the placement of the VM asset to be protected.
- On each ESXi host, the protection-related APIs and workflows from VMware are facilitated using a VAIO filter.
- Each ESXi communicates with the Transparent Snapshot Data Mover (TSDM) component, which is responsible for the VM-backup data movement.
- The backup and restore processes transfer the transparent snapshots respectively to and from the PowerProtect appliance.
- TSDM also consists of the PowerProtect appliance SDK (DD Boost library), which helps the framework access the storage units on the PowerProtect appliance. It also helps write and read data from those storage units.

Note: PowerProtect Data Manager manages the TSDM component by using the VIB (VMware Certified) from Dell Technologies. This component is installed dynamically as part of the integration of PowerProtect Data Manager that requires protection of VMs using transparent snapshots. The APIs being used are supported in VMware ESXi 7.0 U3 and later.

Integration with PowerProtect Data Manager

This section examines the steps to integrate PowerProtect Data Manager within the VMware infrastructure, including deploying all necessary components and enabling VM protection using transparent snapshots.

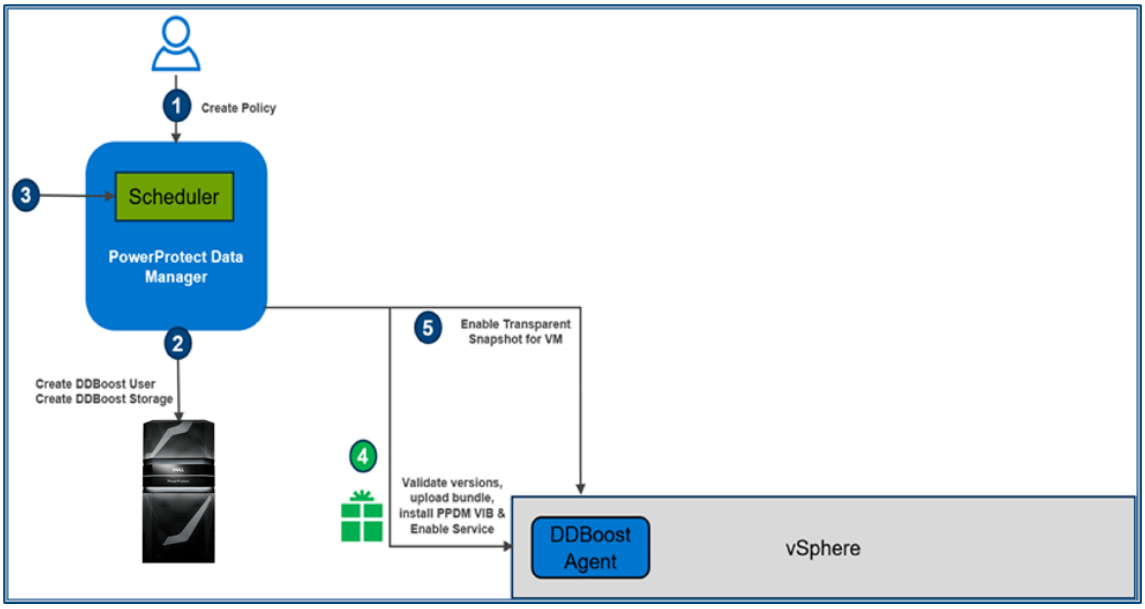


Figure 3. Integration with PowerProtect Data Manager

After VMware VMs are discovered as PowerProtect Data Manager assets, the next steps are creating a protection policy and adding the VM assets for protection.

Note: For information about the criteria for policies to be eligible for transparent snapshots, see Protection Protection Criteria.

---

1. PowerProtect Data Manager creates the storage unit in the PowerProtect appliance for storing backups.
2. According to the schedule defined in the protection policy, the scheduler activates.
3. As these steps occur, the PowerProtect Data Manager VM Direct Engine initiates API calls to vCenter. It then validates the ESXi version (7.0U3 and later), uploads and installs the PowerProtect Data Manager TSDM VIB, and enables the service. Then, the VAIO filter is attached to each VM disk. In this step, the TSDM component is created but remains idle (running but not used) because there is no data movement. You can see the VIB file installed on the ESXi host that houses the VM being protected (Figure 4).

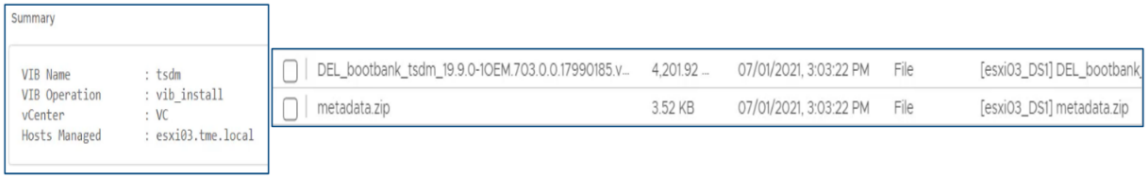


Figure 4. The TSDM VIB file

Note: Installation or upgrade of the TSDM VIB does not require the target ESXi host to be in maintenance mode.

The VIB deployment process operates on the relevant ESXi hosts concurrently—25 ESXi hosts at a time.

The process skips ESXi hosts that are powered off or in maintenance mode. The mechanism also has integrated logic to detect and prevent upload of the VIB package to hosts that already have the package in one of their datastores.

4. When vCenter acknowledges success, PowerProtect Data Manager marks the VM to be protected by transparent snapshots.

Note: Aside from the DEL_bootbank VIB file, Figure 4 shows a metadata.zip file that contains information related to the VIB, such as dependencies on the host, system requirements, summary, and version. The files are in the Datastore Files section of the ESXi host. This VIB installation is also shown in the PowerProtect Data Manager Policy Config Job summary.

Protection Criteria

The criteria for policies to be eligible for transparent snapshots are:

- Crash consistent or application consistent for Microsoft SQL Server (with PowerProtect Data Manager 19.14 and later)
- Performance Optimization mode or Capacity Optimization Mode (with PowerProtect Data Manager version 19.10 and later)
- Swap File Exclusion: Disabled
- Quiesce Filesystem: Disabled

Policies created before PowerProtect Data Manager 19.9 will not automatically start to use TSDM upon upgrade to 19.9 and later. The same is true for policies created in 19.9 or earlier with Capacity Optimization mode: TSDM will not be used automatically upon upgrade to PowerProtect Data Manager 19.10. The Data Mover type would be updated the next time the policy is edited or when it is explicitly configured. When a full backup would be performed for the first time, TSDM operates then and when the policy option is switched between Performance and Capacity Modes. TSDM remains the Data Mover when Performance Optimization mode is switched to Capacity Optimization mode, and conversely.

PowerProtect Data Manager 19.10 enhancements

As a precautionary measure, starting with version 19.10, PowerProtect Data Manager uses VADP automatically in the following cases:

- VM with RDM disks
- VM with more than 40 disks
- VM with Fault Tolerance (FT) enabled

Also, with PowerProtect Data Manager 19.10, backups that are taken with TSDM as the data mover can replicate to the cloud using Cloud DR for all supported cloud protection and recovery use cases.

PowerProtect Data Manager 19.11 enhancements

Beginning with version 19.11, the PowerProtect Data Manager UI provides an option to override the automatic protection engine selection and manually select the VM Direct protection engine to be used. It also enables the option to migrate the protection engine being used on an asset basis. For example, VADP is being used to back up a certain VM and now the backup admin wants to leverage TSDM so the asset protection engine can be migrated to TSDM.

Limitations

As a precautionary measure, PowerProtect Data Manager does not support the following with transparent snapshots:

- Physical or virtual RDM disks.
- VMs with encrypted VMDKs.
- VMs with more than 64 disks (PowerProtect Data Manager).
- VMs with Fault Tolerance (FT) enabled.
- Azure VMware Solution (AVS) on Microsoft Azure.
- VMware Cloud (VMC) on Amazon Web Services (AWS).
- VMware Live Site Recovery (VLSR, formerly known as VMware Site Recovery Manager (SRM)) cannot co-exist with TSDM on the same VMs. See the section PowerProtect Data Manager 19.17 enhancements for more information.
- Shared disks.
- VMs with VMware snapshots (see Protection of VMs with VMware Snapshots).

Override protection engine

The PowerProtect Data Manager UI provides an option to override the automatic protection engine selection and manually select the VM Direct protection engine to be used. It also enables the option to migrate the protection engine being used on an asset basis. For example, VADP is being used to back up a certain VM and now the backup administrator wants to leverage TSDM so that the asset protection engine can be migrated to TSDM.

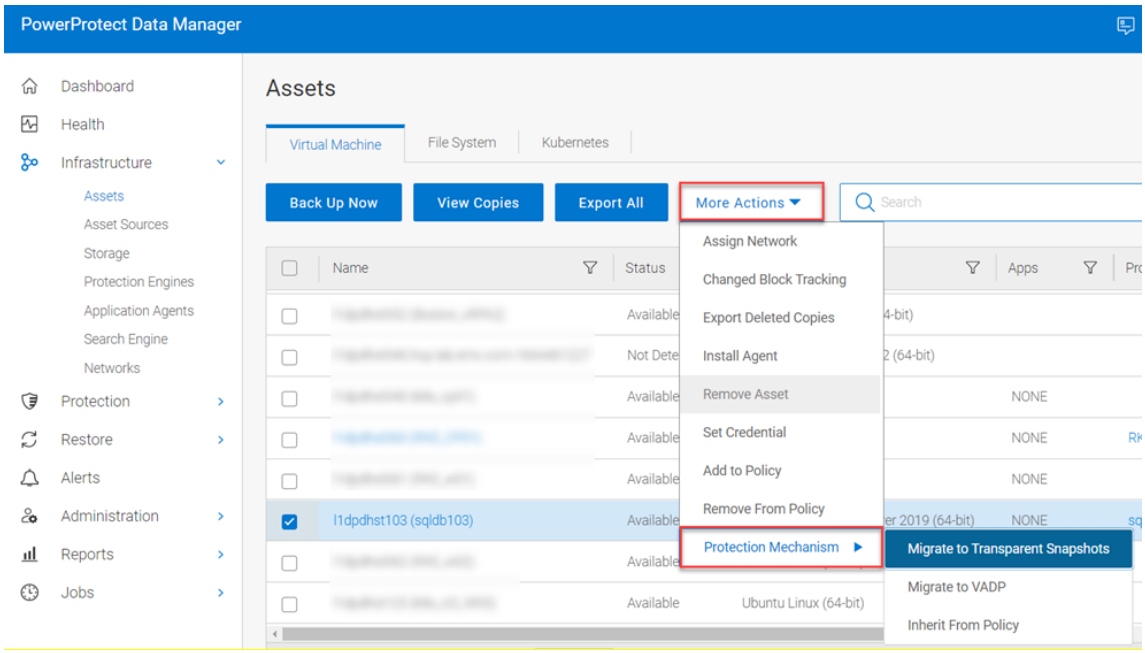


Figure 5. Protection mechanism override

PowerProtect Data Manager 19.12 enhancements

The following features and changes were introduced in version 19.12:

1. The number of concurrent TSDM jobs are doubled to 20 for both backup and restore per ESXi host. In previous releases, the maximum backup and restore jobs were 10 for each type. This new throttling mechanism is available with PowerProtect Data Manager 19.12 and vSphere 7.0U3d and later.
2. VIB deployment enhancements:
   - The VIB deployment process now operates on the relevant ESXi hosts concurrently - 25 ESXi hosts at a time.
   - The VIB deployment process skips ESXi hosts that are powered off or in maintenance mode.
   - The VIB deployment process has been enhanced to prevent upload of the VIB package to hosts that already have the package in one of their datastores.

PowerProtect Data Manager 19.13 enhancements

PowerProtect Data Manager 19.13 introduced the following capabilities:

- **Restore storage policies** - The option to assign, upon restore, the VM and its disks to the set of storage policies assigned at the time of the backup.
- **Backup and restore encrypted VMs (VMcrypt)** - Support for protection of encrypted VMs. Support for encrypted VMs depends not only on PowerProtect Data Manager 19.13 but also on vSphere 8.0 (patch b). An encrypted VM is always backed up as unencrypted. If the restore storage policy option is not selected as part of the restore flow, then the VMDKs would be restored as unencrypted, and the default datastore storage policy would be used. The restored VMDKs would be encrypted and assigned to the VM encryption policy if the option to restore storage policy is selected and the original VM disks were assigned to encryption storage

policy. In such cases, the encryption would be a post-restore action on the vSphere side once the encryption storage policy gets associated with the restored VMDKs.

- **Restore VM BIOS UUID** - An option to restore the VM BIOS UUID at time of backup, for restore to a new VM as well as VM restore using instant access.
- **Restore individual VMDKs** - The ability to restore individual VM disks when restoring back to original or to an alternate VM on the same vCenter or on a different one.

PowerProtect Data Manager 19.14 enhancements

PowerProtect Data Manager 19.14 features many important transparent snapshots-related enhancements:

- **Support for application consistency for Microsoft SQL Server using transparent snapshots** - Application consistency for SQL Server with transparent snapshots is now supported, in addition to the Application Direct offering. SQL Server application-aware backups with TSDM are designed to operate with the embedded VM Direct Engine. Policies that feature SQL Server application-aware VM backups using VADP from previous PowerProtect Data Manager releases are not automatically migrated to TSDM. For more information, see Override protection engine.
- **TSDM VIB life cycle improvements** - The TSDM VIB life cycle had been greatly enhanced in this release. First, an upgrade option is now available in the PowerProtect Data Manager UI as well as through the PowerProtect Data Manager REST API. If an ESXi host is eligible for an upgrade, VIB status for the ESXi host is displayed as **Ready for upgrade**, and the **Upgrade** button is enabled. A message is also displayed to warn against performing upgrades while backups are running.

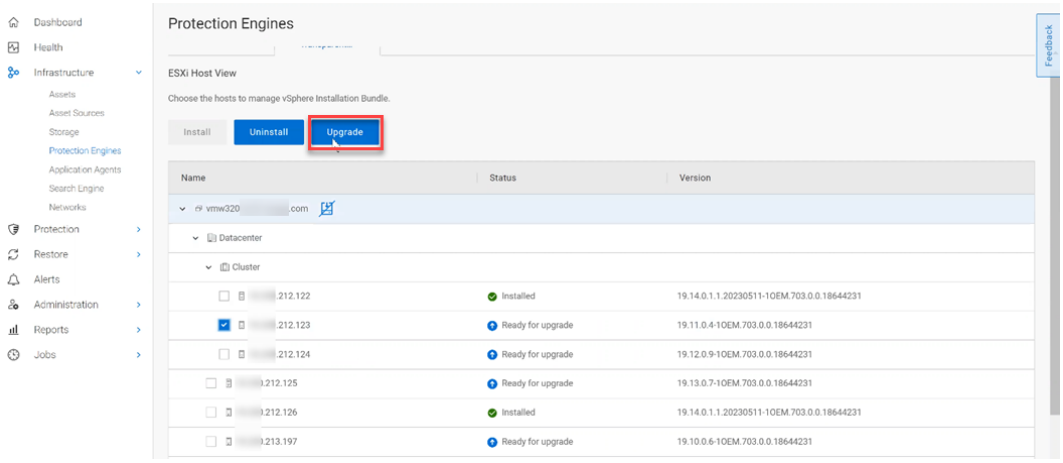


Figure 6. TSDM VIB upgrade option

- **Support for TSDM VIBs with earlier PowerProtect Data Manager releases** - Starting with PowerProtect Data Manager 19.14, TSDM VIBs can run earlier releases of PowerProtect Data Manager, unless stated differently in the PowerProtect Data Manager ESSM for your specific release.
  - When automatic VIB management on a vCenter is disabled, ESXi hosts with VIB version N-4 and later will skip the VIB upgrade during the PowerProtect Data Manager upgrade. N-4 for PowerProtect Data Manager 19.14 means that

PowerProtect Data Manager 19.10 and later releases will not be automatically upgraded.

  - When automatic VIB management is enabled, all ESXi hosts with TSDM VIBs on that vCenter will be automatically upgraded.

- **Support of VM image-based protection on Oracle Cloud VMware Solution (OCVS)** - PowerProtect Data Manager 19.14 supports VM protection on OCVS. Both TSDM and VADP VM image-based protection is supported. PowerProtect Data Manager as well as PowerProtect DDVE can now be deployed on OCVS. Specifically, the PowerProtect Data Manager OVA was enhanced with an additional OCVS deployment option.
- **Policy UI changes for TSDM** - PowerProtect Data Manager 19.14 greatly enhances VM policy configuration by allowing you to explicitly select transparent snapshots (default) or the VADP protection mechanism. The protection mechanism changes are based on the selected backup options (see Criteria).

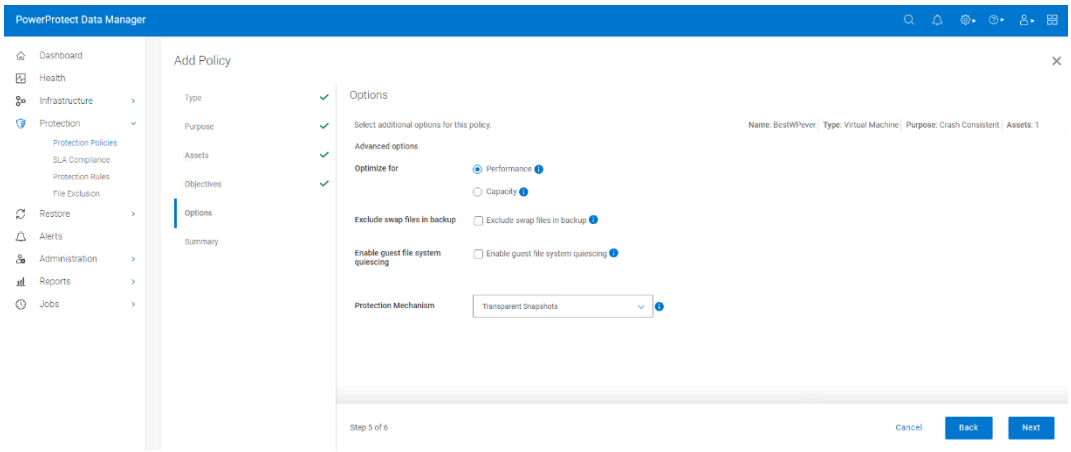


Figure 7. Policy creation flow improvements

- **Restore plans** - Restore plans can now be leveraged to orchestrate mass asset restore operations. Restore plans can be run ad hoc or can be scheduled and restore plans can be reused or repurposed. A restore plan includes one or more restore groups that represent the assets to be restored, by a specific policy, by rule, or by manual selection. The restore group definition also includes copy selection, restore method and location, and network mapping as well as configuration. Restore plan functionality is limited to VM assets in PowerProtect Data Manager 19.14 that were backed up using transparent snapshots or VADP. For more information about restore plans, see the *PowerProtect Data Manager Virtual Machine User Guide*.

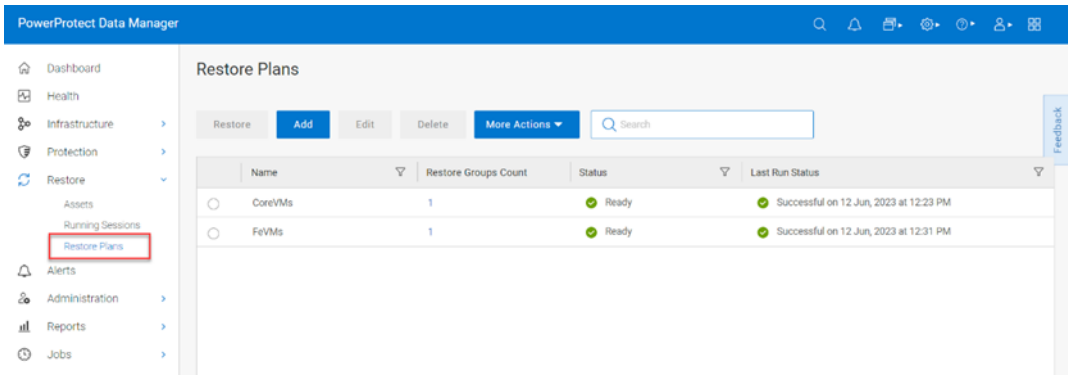


Figure 8. Restore Plans

PowerProtect Data Manager 19.15 enhancements

PowerProtect Data Manager 19.15 introduced the following capabilities:

- **vCenter privileges validation** - when a vCenter is added as an asset source or when an existing vCenter asset source is edited, with PPDM 19.15, it is possible to verify the configured vCenter credentials and meet the minimum required vCenter user account privileges. *PowerProtect Data Manager Virtual Machine User Guide* lists all vCenter privileges necessary for TSDM.

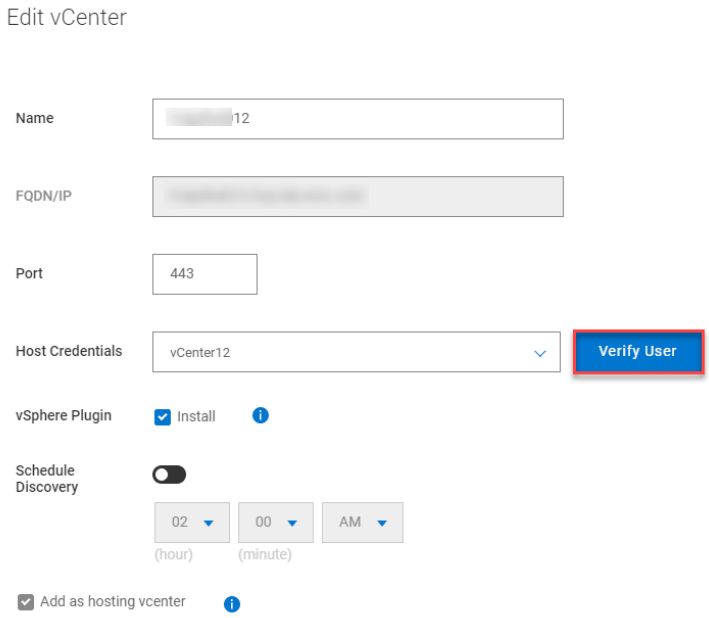


Figure 9. vCenter privileges validation for vCenter asset sources

- **Clone protection policy** - PPDM 19.15 offers the ability to clone an existing protection policy to a new one for simplification and automation. The new policy is created with no assets because only configuration is cloned.

PowerProtect Data Manager 19.16 enhancements

PowerProtect Data Manager 19.16 features these VM-related improvements:

- **Distributed Resource Scheduler (DRS) Support for VM Restore** - this capability enables the selection of an ESX cluster with DRS enabled as the target to run the

recovered VM. This is available for all restore types and the ESX cluster selection is available through the PPDM UI and PPDM vSphere plugin.

Note: upon using restore, individual ESXi hosts must be selected to run the recovered VM. This applies only for clusters with DRS disabled as in previous releases.

- **Copy Management UI** - a brand-new UI screen located under Infrastructure which allows users to view and manage all copies through a single screen. This new capability not only allows users to view copy details, but also allows them to edit the copy retention, delete, or remove the copy from PPDM. Additionally, it enables search (including advanced search) for copies.

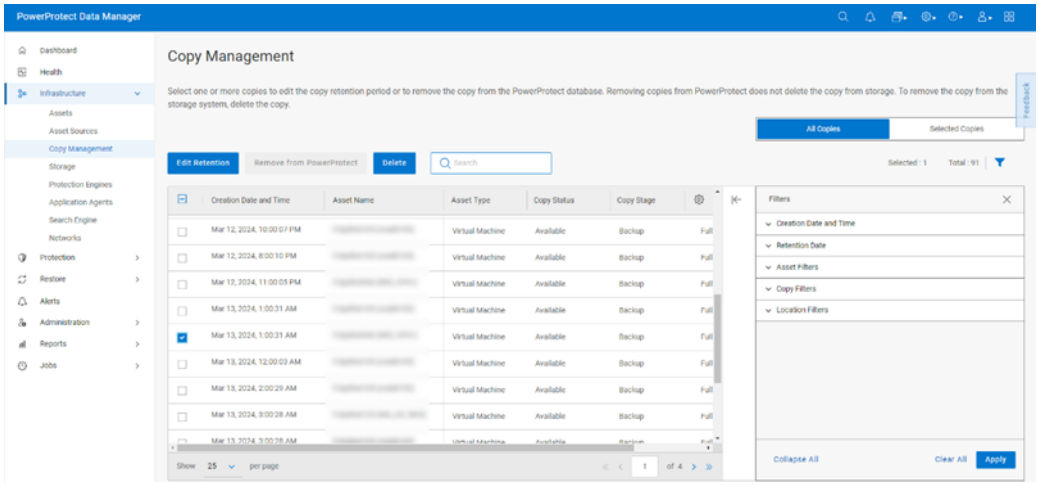


Figure 10. Copy Management UI

- **Restore of Deleted VMs** - VM restore to original has been enhanced to support vCenter, datacenter, ESX cluster, datastore, and others that no longer exist. The PPDM UI tries to pre-select previous existing locations if available; but in any case, the user can change any of these locations and ultimately restore the VM even if the original location is not available. That is done by preserving the VM instance UUID which is advantageous as the backup history is kept for the production or restored VM.

PowerProtect Data Manager 19.17 enhancements

PowerProtect Data Manager 19.17 features support for VMware Live Site Recovery (VLSR, formerly known as Site Recovery Manager (SRM)), specific to Host-Based Replication (HBR) which enables VM-based replication. This means that it is now possible to perform a backup of VMs that are protected by VLSR, using PPDM Transparent Snapshots. This added support relies on VMware Live Site Recovery 9.0.1.

Along the same lines, 19.16 was also qualified and now supports co-existence with VLSR VM-based replication as well.

Note: As the time of publication, VLSR using Array-Based Replication (ABR) cannot co-exist with TSDM.

PowerProtect Data Manager 19.18 enhancements

PowerProtect Data Manager 19.18 features the ability to configure auto-VIB management as part of the vCenter asset source registration or modification flows in the PowerProtect Data Manager UI and REST API. By default, auto VIB management is enabled. Auto-VIB management can be enabled or disabled either through the asset source registration/modification screen or through the Protection Engines -> Transparent Snapshots Data Movers screen (Figure 6).

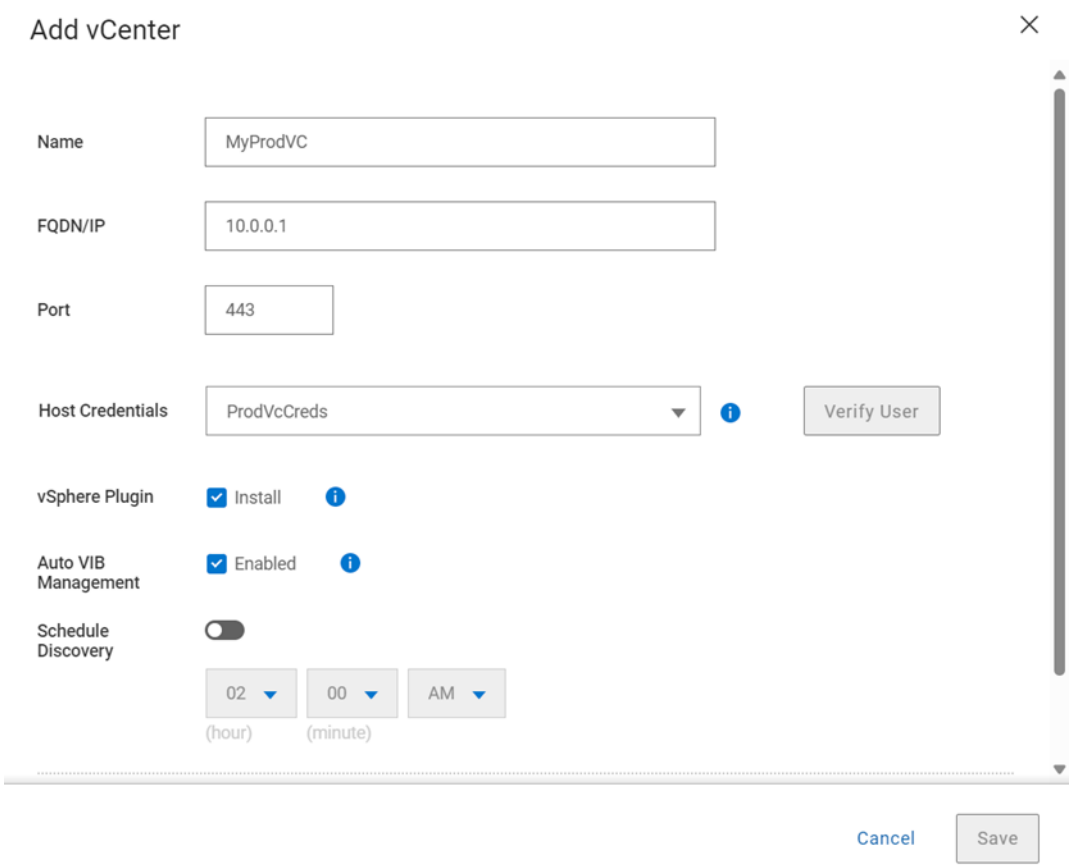


Figure 11. vCenter Asset Source Registration in the PPDM 19.18 UI

PowerProtect Data Manager 19.19 enhancements

- **Manual VMDE Upgrade** - PowerProtect Data Manager 19.19 introduces the ability to disable automatic upgrades for VMware VM Direct Engine (VMDE), allowing administrators to decouple the vProxy lifecycle management from Data Manager upgrades. Automatic VMDE updates can now be controlled on a per-vCenter basis through the Protection Engine UI screen or API, with configuration supported only for vProxies that are on the same version as Data Manager or the previous release. When a VMDE becomes eligible for upgrade, Data Manager generates a system alert to raise awareness and let users plan their VMDE upgrade on their own schedule.
- **Google Cloud VMware Engine (GCVE) Support** - PowerProtect Data Manager 19.19 adds support for backing up and restoring virtual machines running on Google Cloud VMware Engine (GCVE) using Transparent Snapshots. This capability requires specific vCenter privileges for the service account used by Data Manager, which are

documented in the PowerProtect Data Manager VMware VM User Guide. In this release, protection for GCVE workloads is limited to crash-consistent copies.

- **Anomaly Detection** - PowerProtect Data Manager 19.19 features anomaly detection for vSphere VM workloads, generating reports when it identifies unusual patterns in backup metadata that may indicate security concerns. This capability requires the data to be indexed and the search engine to be deployed, since detection runs against indexed metadata rather than full backup content. When anomalies are found, the resulting reports can be used to quarantine or delete the affected backup copies to prevent potentially compromised data from being restored.

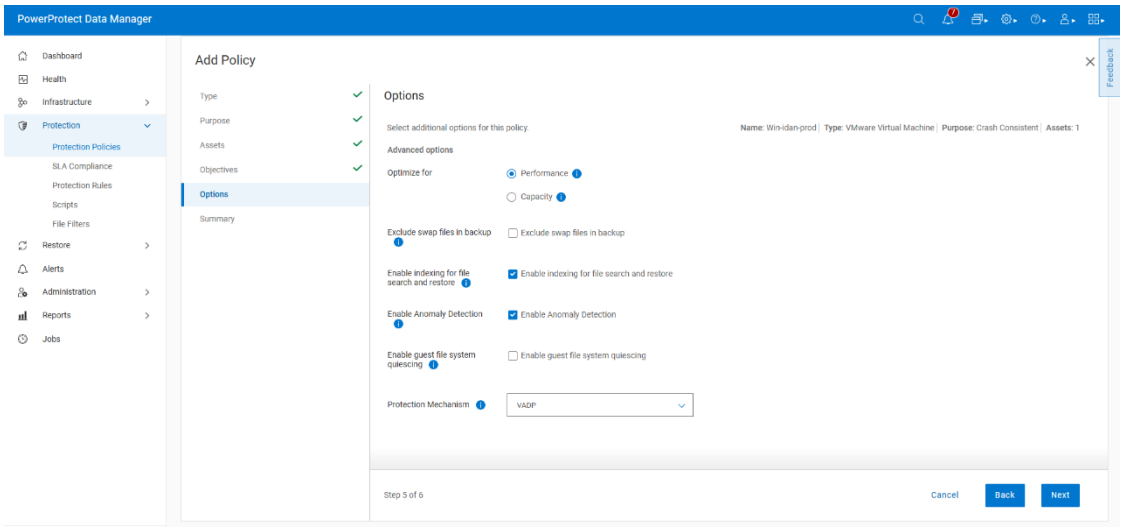


Figure 12. Updated Protection Policy options with Anomaly Detection

PowerProtect Data Manager 19.20 enhancements

- **vProxy Precheck Enhancements** - PowerProtect Data Manager 19.20 adds the ability to run protection engine upgrade prechecks for VM vProxies at the vCenter level, and it allows both prechecks and upgrades to be performed on across vCenter servers.
- **TSDM Support for VMs with high disk count** - Data Manager 19.20 introduces TSDM support for protecting and restoring VMs with more than 40 VMDKs, which previously required VADP. The release enables TSDM to process large-disk VMs by opening VMDKs in batches based on stream count and ESXi memory, and it raises the guardrail from 40 to 64 VMDKs.

PowerProtect Data Manager 19.21 enhancements

Starting with 19.21, PowerProtect Data Manager adds low-privilege backup and restore operator roles that let organizations assign specific backup and restore responsibilities without granting full administrative access.

- **Backup Operator** - The Backup Operator role is responsible for running manual backup operations. Users in this role work only with resources that an administrator has already configured. They can back up assets and monitor backup jobs, but they cannot manage backup policies or infrastructure.
- **Restore Operator** - The Restore Operator role focuses on performing on-demand restores. These users work with existing backups and the resources

already set up by the administrator. They cannot manage hosts, restore scripts, or restore plans.

PowerProtect Data Manager 19.22 enhancements

- **vSphere 9.0 Support** – PowerProtect Data Manager 19.22 introduces guardrails for environments running vSphere 9.0. Although vSphere 9.0 continues to be supported through VADP (starting in Data Manager 19.21), it is not supported with Transparent Snapshots. When vSphere 9.0 is detected, Data Manager automatically reverts to VADP for VMware VM protection.

  Guardrails introduced in 19.22 for vSphere 9.0 include:

  - Automatic fallback to VADP - When vSphere 9.0 is detected, Data Manager automatically switches the protection mechanism defined in the protection policy to VADP.
  - Warnings for incompatible protection policies - If a protection policy is configured to use Transparent Snapshots for assets on asset sources upgraded to vSphere 9.0, Data Manager displays warnings indicating that Transparent Snapshots are not supported.
  - TSDM VIB marked as not eligible - On ESXi hosts running vSphere 9.0, the TSDM VIB is automatically set to not eligible, preventing any VIB related operations from being executed through the PowerProtect Data Manager UI and API.

- **Compatibility with older vSphere releases -** PowerProtect Data Manager aligns with the vSphere support lifecycle. Therefore, it no longer supports vSphere versions earlier than 8.0 for VM protection or deployment

PowerProtect Data Manager 20.1 enhancements

- **Interactive workflow map** - PowerProtect Data Manager introduces an interactive workflow map that helps visualize all key asset information within a single screen in the PowerProtect Data Manager UI. Administrators can view the asset source, complete policy configuration, protection storage details, recent copies, and the most recent restore activity in one place.

- **Honor SQL AAG backup preference for TSDM application-consistent full backups** - PowerProtect Data Manager 20.1 and later honors SQL Always On Availability Group backup preferences for application-consistent full backups. The selected preferred replica is used for the snapshot while non-preferred replicas skip the database, ensuring full-backup behavior aligns with the SQL AAG backup preference.

Protection parallelism

With vSphere 7.0U3d and later, there can be a maximum of 20 concurrent jobs - backups and restores - per ESXi host. The limit is set to 18 concurrent backup jobs or 16 concurrent restore jobs per host. It is a shared pool in which neither backup nor restores can reach 20, so that other restore and backup jobs can run at the same time.

With vSphere 7.0U3c, there is a static limit of 10 concurrent backup jobs and 10 concurrent restore jobs per ESXi host.

There can be maximum of 180 concurrent VM operations per vCenter.

Network considerations

TSDM requires connectivity to PowerProtect Data Domain for data path purposes (see various flows described in

Furthermore, the PowerProtect Data Manager REST API documentation on the Dell Developer Portal also features a tutorial on how to upgrade the TSDM VIB on ESXi hosts and clusters.

Transparent snapshots life cycle). This communication is facilitated using VMKernel (VMK) ports on the ESXi hosts where the TSDM VIB is installed. The transparent snapshots solution would work outside of the box without dedication of VMK ports because any VMK port that can communicate with PowerProtect DD would be automatically used.

That said, for optimal predicted performance and scale, the following guidelines are recommended:

- **Dedicated VMK ports**: Create a single dedicated VMK port per ESXi host. Having a dedicated VMK port decreases the chances of performance degradation due to sharing of VMK ports with other consumers, especially vMotion and vSAN.
- **VMK ports placement**: We recommended placing the VMK port on a VLAN that is dedicated for TSDM to PowerProtect DD traffic or a VLAN dedicated for backup traffic. Having the VMK ports and the relevant PowerProtect DD ports on the same L2 network (same broadcast domain) is advised. Avoid placing the VMK ports and PowerProtect DD ports on VLANs with heavy burst traffic such as vMotion, iSCSI networks, or FT.
- **Consistent end-to-end MTU**: Ensure that the MTU set on the VMK port and on the PowerProtect DD port is uniform from end to end. You can validate this setting by running the ESXCLI command `vmkping` with the DF flag. For example, the following command checks whether there is a uniform end-to-end jumbo frame through a specific VMK port:

  ```
  vmkping -I vmk1 -d -s 8972 10.10.100.1
  ```

Essential firewall ports

The following table outlines the main necessary firewall ports for Transparent Snapshots.

Table 1. Outline of TSDM required firewall ports

Source	Destination	Port	Protocol	Comments
PowerProtect Data Manager	vCenter	443	TCP	
PowerProtect Data Manager	vCenter	7444	Proprietary	
PowerProtect Data Manager	ESXi	443	HTTPS	
PowerProtect Data Manager	Protection Engine	9613	Proprietary	External VMDE only
PowerProtect Data Manager	Protection Engine	22	TCP	External VMDE only

Source	Destination	Port	Protocol	Comments
PowerProtect Data Manager	Protection Engine	9090	HTTPS	External VMDE only
PowerProtect Data Manager	PowerProtect DD	3009	HTTPS	Embedded or external VMDE
PowerProtect Data Manager	PowerProtect DD	111	TCP	Embedded or external VMDE
PowerProtect Data Manager	PowerProtect DD	2049	TCP	Embedded or external VMDE
PowerProtect Data Manager	PowerProtect DD	2052	TCP	Embedded or external VMDE
ESXi	PowerProtect DD	111	TCP	Embedded or external VMDE
ESXi	PowerProtect DD	2049	TCP	Embedded or external VMDE
ESXi	PowerProtect DD	2053	TCP	Embedded or external VMDE

Upon installation of the TSDM VIB, a service called daemon-tsdm is added to the ESXi firewall. This ruleset includes the following properties.

Table 2. TSDM firewall ruleset

Service Name	Incoming Port	Outgoing Port	Protocol	Allowed IP addresses
daemon-tsdm	N/A	111	TCP	All (default). Can be configured as needed
daemon-tsdm	N/A	2049	TCP	All (default). Can be configured as needed
daemon-tsdm	N/A	2053	TCP	All (default). Can be configured as needed

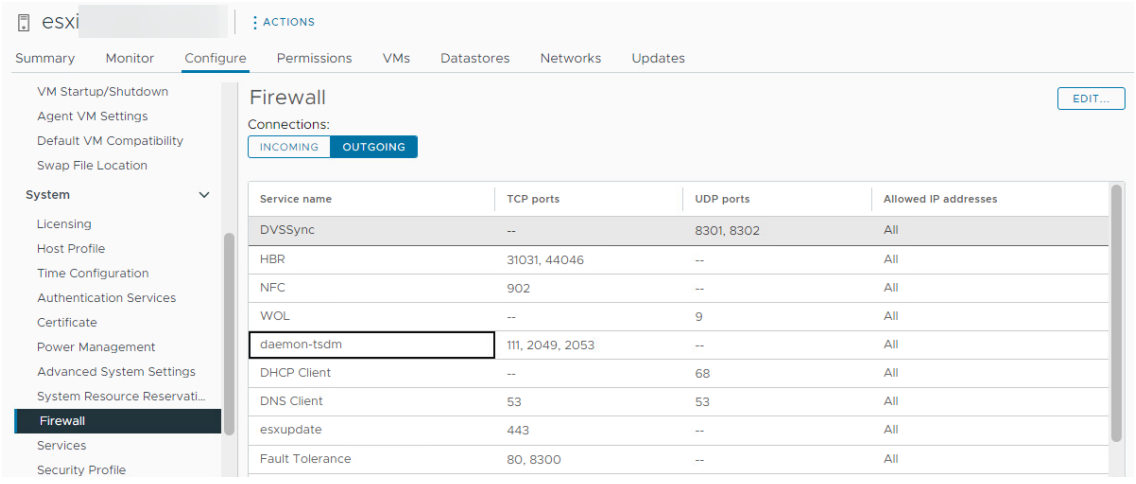


Figure 13. Outline of TSDM required firewall ports

TSDM supports ESXi Lockdown Mode. To ensure the successful creation of the daemon-tsdm firewall ruleset during VIB installation, it is required to add root as an exception user. As a matter of fact, in PPDM 19.17 and later, VIB installation would fail if Lockdown Mode is enabled without root as an exception user.

For additional security-related information, see the *PowerProtect Data Manager Security Configuration Guide*

VM Direct Engine considerations

The VM Direct Engine (VMDE) runs on the PPDM VM itself and it is available for TSDM operations without having to perform any specific configuration. In terms of scale, TSDM supports up to 180 concurrent VM backups. This embedded VMDE is suitable for most TSDM use cases.

External VMDE can be used with TSDM for cases where 300 concurrent VM backups and a scale of up to 5000 VMs with multiple vCenter servers are required.

Protection of VMs with VMware Snapshots

Protection of VMs with VMware snapshots (or managed snapshots) is not supported for VM backups using Transparent Snapshots. Once a VM is configured for Transparent Snapshots, then the VM snapshots can be created without any impact to TSDM backup and restore operations. In vSphere 7.0U3, a TSDM backup job that is running on a VM with managed snapshots would fail with a *CancelSnapshotRequired* error. In vSphere 8.0 and later, the TSDM protection configuration job would fail with the following error: *"SPIF filters change failure: One of the parameters supplied is invalid. The IO Filter policy cannot be changed when snapshot disks are present*".

vSphere Interoperability

- PowerProtect Data Manager 19.22 and later support Transparent Snapshots when used with vSphere 8.0, including 8.0 U3 and all subsequent patches.
- Data Manager 19.21 supports vSphere 7.0 U3c and later, including vSphere 8.0 U3, but only for VADP backups.
- Transparent Snapshots are not supported with Data Manager 19.21 on vSphere 8.x.
- vSphere 9.0 is supported by Data Manager 19.21 and later, but only with VADP.
  - Transparent Snapshots are not supported with any Data Manager version on vSphere 9.0.
  - Guardrails are introduced in Data Manager 19.22

The PowerProtect Data Manager Compatibility Matrix exists for the each respective PowerProtect Data Manager release, contains up-to-date interoperability information on vSphere support and more.

TSDM-specific REST API calls

PowerProtect Data Manager features specific REST API calls for TSDM VIB Management. The following table summarizes these API calls

Table 3. TSDM VIB management API calls

API HTTP Method	API Endpoint	Purpose	Developer Portal	Comments
GET	/api/v2/vib-details	Get all VIB details	Developer Portal - PPDM API Documentation	
POST	/api/v2/vib-install-batch	Deploy VIB	Developer Portal - PPDM API Documentation	Deploy the TSDM VIB on one or more ESXi hosts and/or clusters
POST	/api/v2/vib-uninstall-batch	Uninstall VIB	Developer Portal - PPDM API Documentation	Uninstall the TSDM VIB on one or more ESXi hosts and/or clusters
POST	/api/v2/vib-upgrade-batch	Upgrade VIB	Developer Portal - PPDM API Documentation	Upgrade the TSDM VIB on one or more ESXi hosts and/or clusters

Furthermore, the PowerProtect Data Manager REST API documentation on the Dell Developer Portal also features a tutorial on how to upgrade the TSDM VIB on ESXi hosts and clusters.

Transparent snapshots life cycle

Transparent snapshots provide for a simple, fast, and efficient VM backup. The high-level life cycle is as follows:

- Monitor: Track delta changes in memory
- Process: Transfer delta changes directly to protection storage
- Release: Remove delta table and any temporary data blocks

To provide a better understanding of the VM backup process, this section describes the synchronization and data transfer process, which consists of four major steps:

- Full sync
- Transparent Snapshot creation
- Delta sync
- Snapshot retire

Full sync operation

The full sync operation process, as shown in Figure 14, is as follows:

1. PowerProtect Data Manager issues a full sync request. This request includes all required parameters such as VM information, disk inclusion details, and disk exclusion details.
2. PowerProtect Data Manager queries vCenter to locate the relevant ESXi host, and the operation is transferred to the ESXi host.

3. The ESXi host synchronizes with the TSDM component, leverages VAIO, and makes TSDM aware that a full sync should be performed on the specific asset.
4. TSDM first uses VAIO to read and query the allocated areas of the disks. After resolving the allocated areas, the TSDM starts to read the data.
5. TSDM also uses the DD Boost library to establish a connection to the PowerProtect appliance. Empty files are created in the secondary storage (each file corresponding to the flat VMDK file of the VM asset), and the data transfer begins. Eventually, all allocated areas are transferred and written to the PowerProtect appliance.
6. When the full sync operation is complete, the TSDM sends an acknowledgment to the ESXi host. vCenter marks the task as complete.

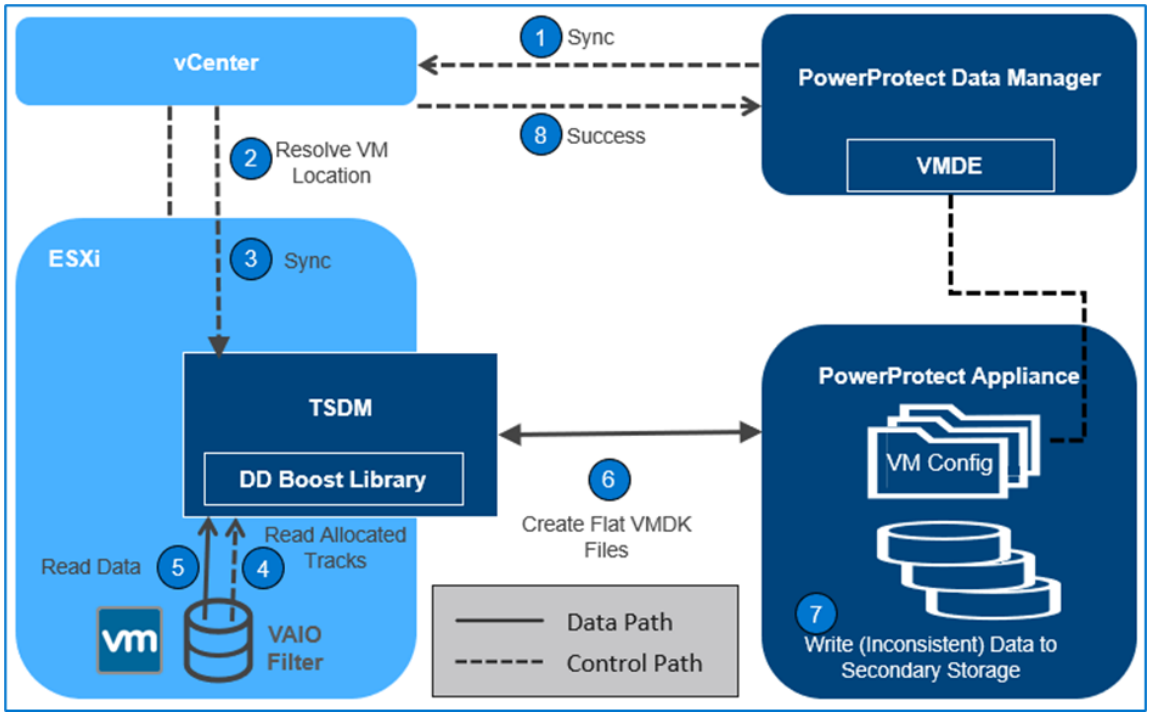


Figure 14. Full sync operation

Note: Because files created during the full sync flow are inconsistent, you cannot use them to restore the VM to a consistent point in time. During the full sync flow, the VM still serves I/O operations, and data in disks might change during the full sync operation itself. A delta sync operation must be performed right after the full sync operation, which creates a consistent point-in-time copy that can be used later for a restore operation.

Transparent snapshots creation

The transparent snapshots creation process (Figure 15) is as follows:

1. After the full sync is complete, PowerProtect Data Manager issues a snapshot creation operation.
2. PowerProtect Data Manager requests a sync operation against vCenter.
3. The API calls are passed to the ESXi host after the location is resolved. In this step, the TSDM has no active role because no data transfer occurs.

4. The ESXi host communicates with the relevant VM asset using VAIO, and the snapshot is persisted to the Snapshot Extent Store (SES).

   Note: The Snapshot Extent Store (SES) is dynamically created during snapshot creation and is deleted when the snapshot is retired. The SES stores the bitmaps that correspond to the data in the disk at that time. The SES uses thin-allocated space across the overall datastore space and does not affect the specific VM quota.

5. Using the SES, the VAIO filter takes the bitmap in memory and saves it. Because all of it is bitmap-based, creating the transparent snapshot is fast, which reduces the read/write latency.
6. After the bitmap is persisted to disk, the filter can start tracking changes on the disk again, using a new bitmap.
7. The snapshot operation is marked as finished. PowerProtect Data Manager can use the V M Direct Engine to access the vCenter level task completion and get the snapshot UUID that was created.

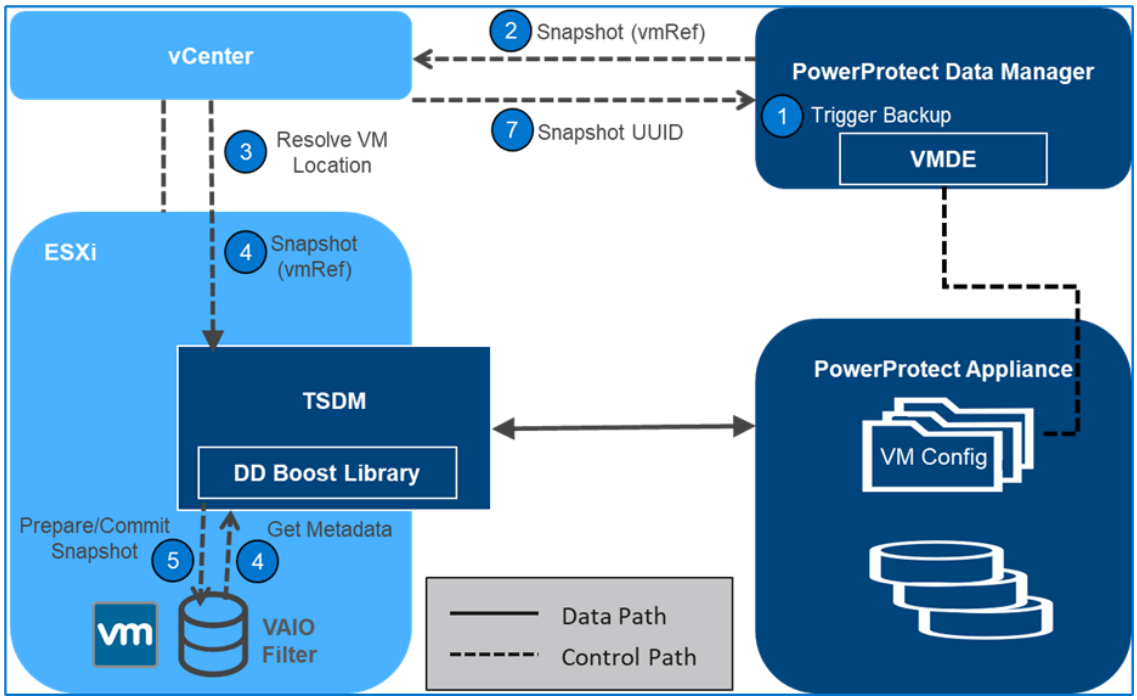


Figure 15. Transparent snapshot creation

Delta sync operation

After the transparent snapshot creation operation is complete, you can initiate a delta sync operation or an incremental operation (see Figure 16). The process is as follows:

1. PowerProtect Data Manager issues API calls to vCenter for a delta sync operation and provides the previously created snapshot UUID.
2. PowerProtect Data Manager signals TSDM to start the delta sync flow through vCenter API, which resolves the relevant ESXi host.
3. The TSDM uses VAIO APIs to query and track the changed areas that the transparent snapshot bitmap represents.
4. For each changed area, the data is read from the disk.

Note: The delta sync operation uses a Fast Copy overwrite approach. In this approach, the previous point-in-time files are first fast copied. The fast-copied files are partly overwritten with incremental data. Only the delta or changes that are represented by the currently synced snapshot are copied. These changes are copied in the Snapshot Extent Store (SES).

5. The changed data or delta is read from the disks to create a consistent data flow.
6. The read data is written to protection storage using the DD Boost library.
7. The changed data write to protection or secondary storage is now complete.
8. When all data has moved to protection storage, the TSDM sends an acknowledgment to the ESXi host that the operation is complete. The vCenter level task is marked as complete.
9. The metadata is written to protection storage. In this step, the VM metadata (such as VMX files, manifest, and the last TSDM snapshot information) is transferred using the VM Direct Engine VMware APIs.

Note: From this point in time, the files on the PowerProtect appliance are crash consistent and can be used for recovery. For a full backup, both full sync and delta sync are performed. However, for an incremental backup, only delta sync is performed. A full sync can back up four VM disks in parallel; a delta sync can back up 10 VM disks in parallel.

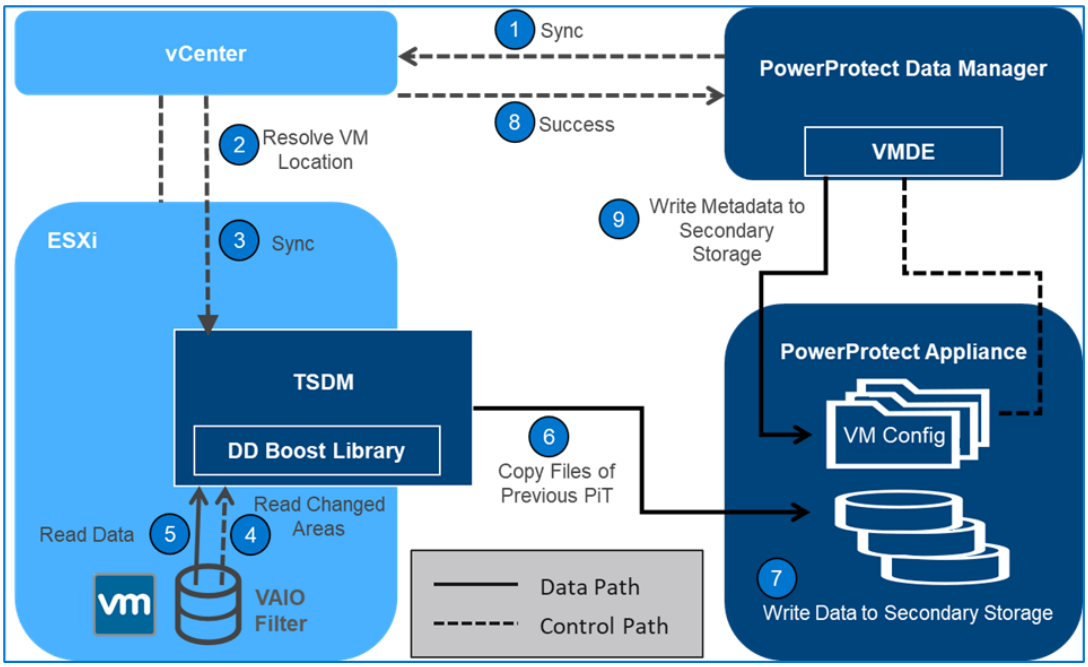


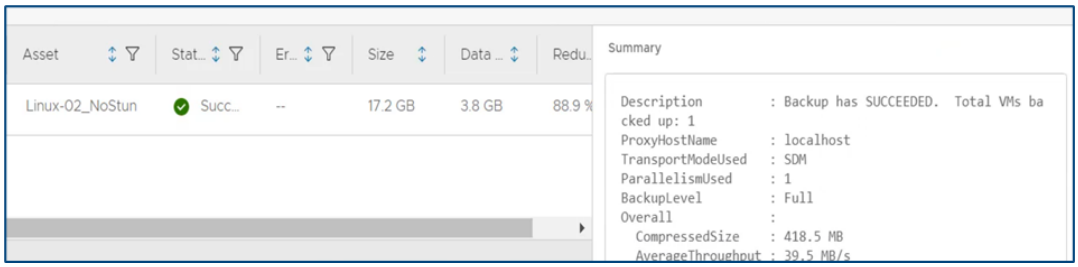
Figure 16. Delta sync operation

Snapshot retire operation

After the delta sync operation is complete, PowerProtect Data Manager ensures that the previously created snapshot is deleted. The snapshot retire operation process (Figure 17) is as follows:

1. PowerProtect Data Manager calls on vCenter to invoke the retire snapshot API towards the relevant ESXi host.

2. The ESXi host relays this information to all the relevant VAIO filters to delete all the bitmaps and copy-on-write data residue left from the snapshot creation and delta sync stages.
3. The ESXi host sends an acknowledgment of the successful snapshot retire operation to vCenter and PowerProtect Data Manager.
4. PowerProtect Data Manager records the backup copy set information in the PowerProtect Data Manager Catalog and informs the search node (if any) to start gathering metadata for indexing.



Notes:

- Transparent snapshots are supported on VMFS, NFS, and vSAN datastores, as well as vVols.
- Virtual and physical RDM volumes are not supported with transparent snapshots.

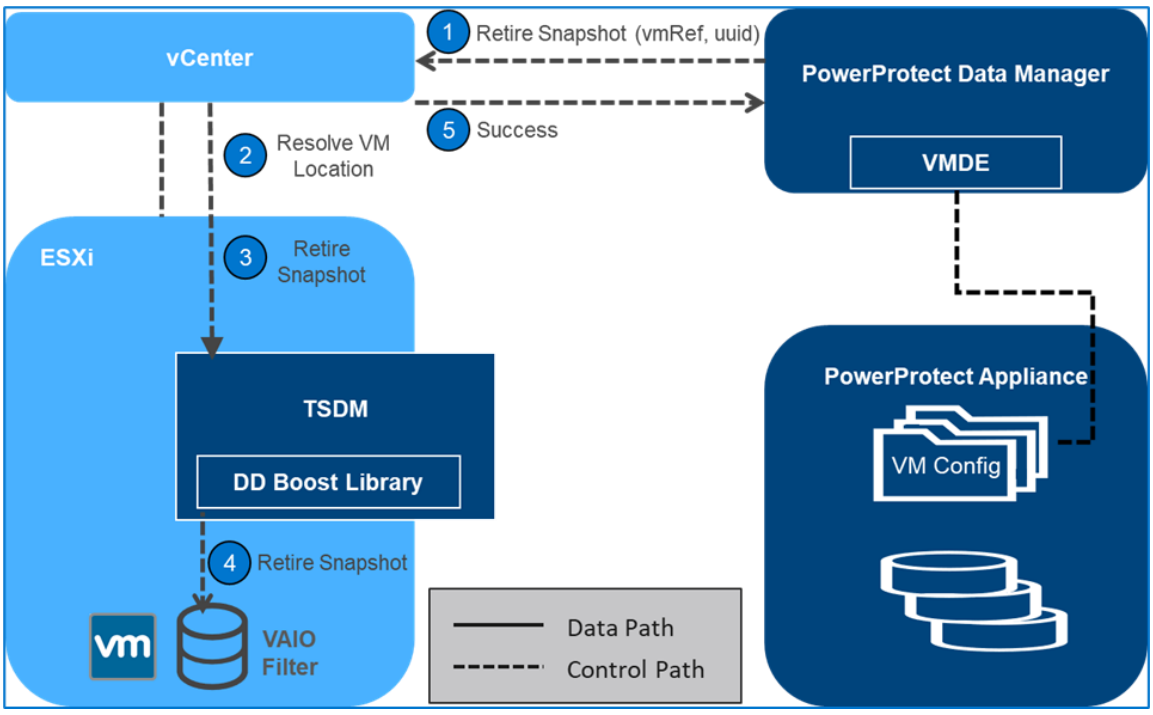


Figure 17. Snapshot retire operation

Restoring virtual machines

Before invoking any APIs from PowerProtect Data Manager to vCenter, PowerProtect Data Manager takes care of the configuration of the VM. For example, if a disk should be added or removed because the VM changed after the snapshot was taken, the disk might

be added. For this reason, the reconfiguration part is performed before the virtual machine is restored.

The virtual machine restore process (Figure 18) is as follows:

1. A metadata-only snapshot is taken using the same snapshot creation flow described in Transparent snapshots creation.
2. PowerProtect Data Manager invokes the restore operation, directing which VM should be restored to what point in time.
3. The VM is checked to determine whether it is in a powered off state. If it is not, the VM is powered off.
4. PowerProtect Data Manager locates the relevant ESXi host through vCenter, and the ESXi host communicates with the TSDM daemon to initiate a restore operation.
5. For a restore workflow, first reserve all the areas of the VM disks that should be reverted to the previous point in time, for the following reasons:
   - To minimize the data you transfer from the protection storage back to the disk
   - To identify which parts of each disk have changed since the point in time to which we are trying to revert to
6. To resolve the previously described changes, the restore workflow leverages two Get Diff APIs, namely Get VAIO Diff API and DD Get Diff API.
7. The ESXi host resolves the Get VAIO Diff API. This difference includes the changes that the VM has made to the disks since the last point in time that was previously synced or backed up to the PowerProtect appliance. The VAIO Diff uses the metadata only snapshot, taken before the VM was powered off, to get the details on what was never written to the PowerProtect appliance.
8. The DD Get Diff API provides the delta details between the last sync point-in-time and the one to revert. It also merges the delta with the delta returned from the previous step. This step provides the complete set of extents that can now be read from the PowerProtect appliance.
9. From the point-in-time copy to which the user wants to revert, data is read and then finally written on top of the VMDKs.
10. After all the data movement is complete, the TSDM sends an acknowledgment to the ESXi host that the restore process has been completed.
11. vCenter marks the task completed and sends an acknowledgment to PowerProtect Data Manager for catalog update.
12. The VM can now be powered on and should have been successfully reverted to the previous point in time.
13. The metadata only snapshot can now be retired, in the same manner as after every delta sync operation.

Notes:

- Multiple streams are opened on the TSDM (when ESXi receives the request) to achieve restore parallelism. You can achieve a higher level of parallelism if the VMs are spread across multiple ESXi hosts.

- Restore in parallel supports up to eight disks of a VM using transparent snapshots.
- Instant access and File Level Restore do not use a specific data mover; hence, they are supported for TSDM-based backups.

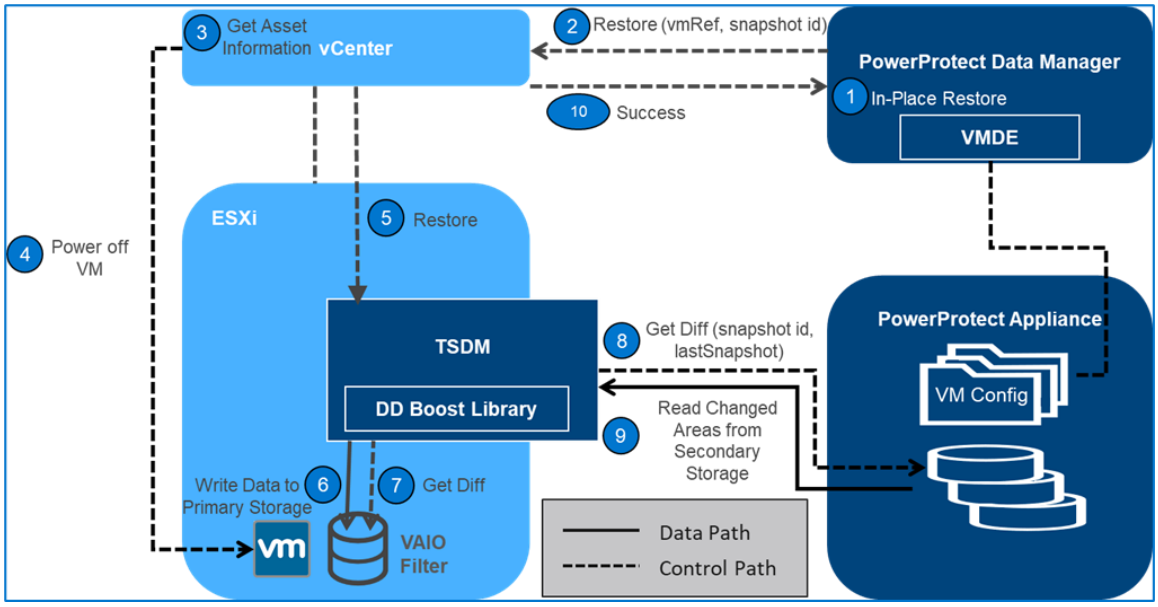


Figure 18. Restoring virtual machines

Performance test results

This section compares the I/O characterization between VMware vSphere Storage APIs - Data Protection (VADP) and transparent snapshots using PowerProtect Data Manager 19.9. You can infer from these results that with transparent snapshots, you overcome the penalties of the write and the read latencies. This result can reduce VM latency by up to five times and provide up to five times faster backups.

Disclaimer: These results compare PowerProtect Data Manager 19.9 with transparent snapshots backup performance (performance-optimized mode) to PowerProtect Data Manager with VADP backup performance. The results are based on Dell Technologies internal testing in August 2021.

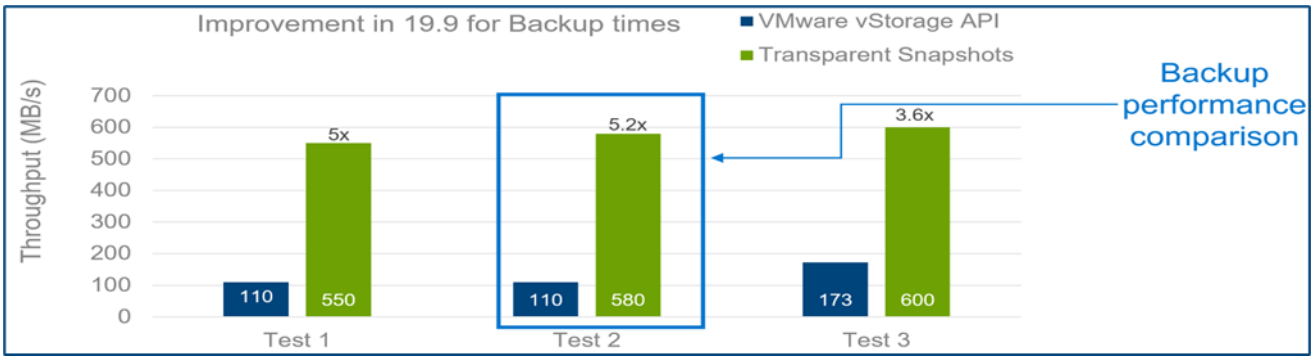


Figure 19. Backup performance comparison

	Transparent Snapshot	VADP
Test 1	**Effective IOPS during Sync:** AVR - **10K** **Sync transfer rate:** AVR - **550 MB/s** **Latency:** During Sync: AVR - **1 ms** No Sync: AVR - **0.5 ms**	**Effective IOPS during Sync:** AVR - **10K** **Sync transfer rate:** AVR - **110 MB/s** **Latency:** During Sync: AVR - **Read: 1 ms / Write: 2.2 ms** No Sync: AVR - **0.5 ms**
Test 2	**Effective IOPS during Sync:** AVR - **10K** **Sync transfer rate:** AVR - **580 MB/s** **Latency:** During Sync: AVR - **1 ms** No Sync: AVR - **0.5 ms**	**Effective IOPS during Sync:** AVR - **10K** **Sync transfer rate:** AVR - **110 MB/s** **Latency:** During Sync: AVR - **Read: 1 ms / Write: 2 ms** No Sync: AVR - **0.5 ms**
Test 3	**Effective IOPS during Sync:** AVR - **10K** **Sync transfer rate:** AVR - **610 MB/s** **Latency:** During Sync: AVR - **1 ms** No Sync: AVR - **0.5 ms**	**Effective IOPS during Sync:** AVR - **10K** **Sync transfer rate:** AVR - **173 MB/s with 12 DD Streams** **Latency:** During Sync: AVR - **Read: 1.1 ms / Write: 2.5 ms** No Sync: AVR - **0.5 ms**

Backup performance comparison

Figure 20. Backup performance comparison test details

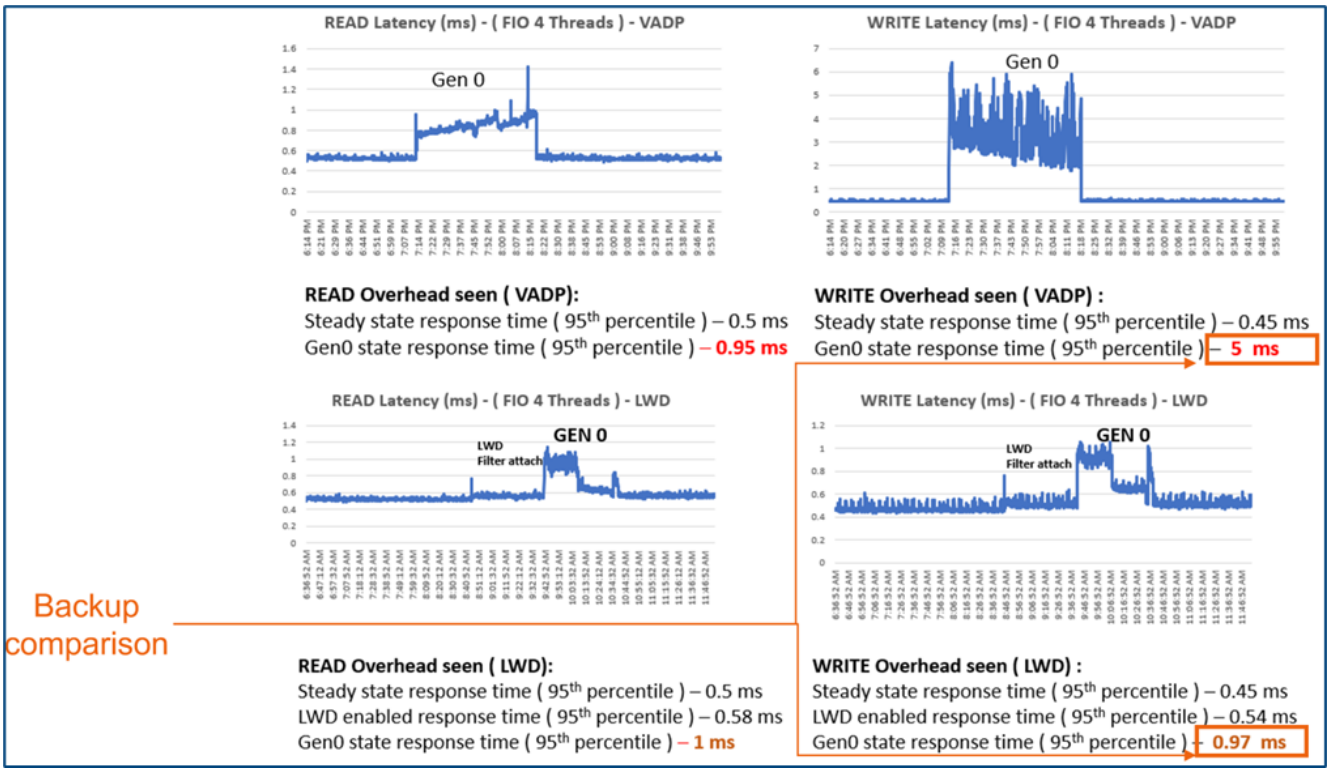


Figure 21. VM latency (read and write) performance comparison

Restore performance

The following results show the restore performance improvements of PowerProtect Data Manager 19.10, as compared to PowerProtect Data Manager 19.9.

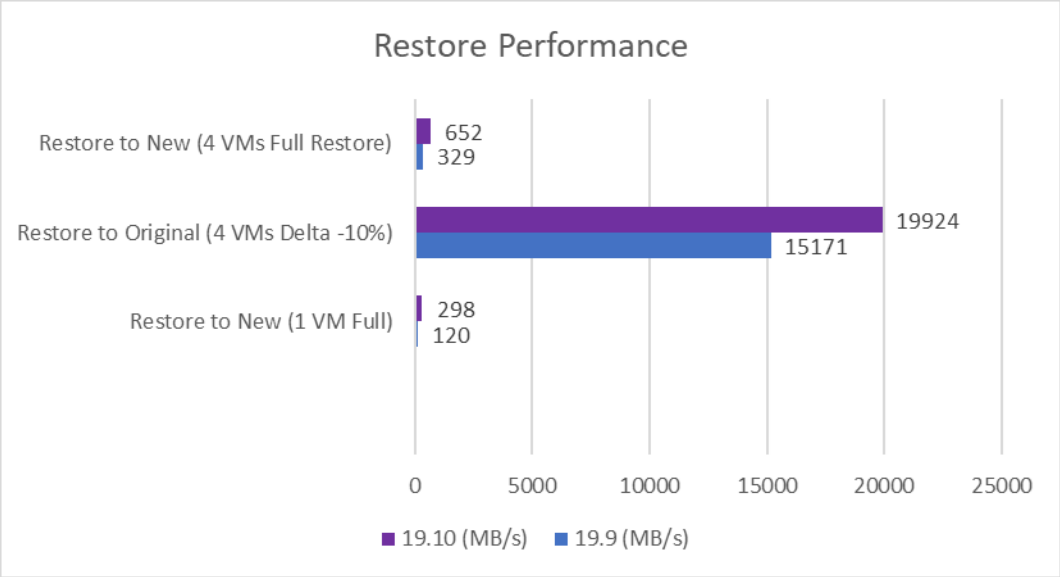


Figure 22. Restore performance comparison

Test	19.9 Throughput (MB/s)	19.10 Throughput (MB/s)	% Improvement
Restore to New (1 VM Full)	120	298	148.3
Restore to Original (4 VMs Delta -10%)	15171	19924	31.3
Restore to New (4 VMs Full Restore)	329	652	98.2

Figure 23. Restore performance comparison test details

References

Dell Technologies documentation

The following Dell Technologies documentation provides other information related to this document. Access to these documents depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.

- PowerProtect Data Manager Interactive Demo
- PowerProtect Official Documentation
- PowerProtect Data Manager at InfoHub
- PowerProtect Data Manager Compatibility Matrices

VMware documentation

See also the following VMware documentation.

- VMware vSphere APIs for I/O Filtering (VAIO)