DELL EMC

Technical White Paper

Dell EMC PowerProtect Software: VMware Backup and Recovery

Abstract

This white paper focuses on the integration of VM with Dell EMC PowerProtect Software and explains the steps required to add an instance of vCenter, create vProxy engines, create protection policies for the virtual machines and how to restore virtual machines using backup copies with PowerProtect Software.

July 2019

Revisions

Date	Description
July 2019	Initial release

Acknowledgements

This paper was produced by the following:

Author: Vinod Kumaresan

Table of Contents

Revisions 2
Acknowledgements 2
Introduction 4
Audience 4
1 Architecture 5
1.1.1 Transport modes: 5
1.1.2 Internal VM proxy engine: 5
1.1.3 External VM proxy engine 6
1.1.4 VM consistent backup 7
1.1.5 Application Application-Aware backup 7
2 Deployment Requirements 8
2.1 Requirements for Application Aware backups on virtual machines 8
3 vCenter authentication 9
3.1 VADP snapshot 9
4 VM Consistent backup configuration workflow 10
4.1 VM consistent backup protection workflow 10
4.2 Application-aware backup configuration workflow 10
4.3 Application-aware backup protection workflow (FULL) 11
4.4 Application-aware backup workflow (LOG) 12
5 Dell EMC PowerProtect Software use-cases for virtual machine recovery 13
6 Disaster Recovery 17
Conclusion 18
References 18

Introduction

Dell EMC PowerProtect Software integration with virtual machines, We can manage, protect, and reuse virtual machine data across the enterprise by deploying services to accomplish the following tasks:

- Discover, access and recover virtual machine copies non-disruptively across primary and protection storage without introducing new infrastructure or complexity
- Automate efficient copy creation
- Efficiently automate data retention SLA compliance, ensuring that the right number of copies are stored in the right place at the right level of protection
- Optimize operations based on actionable analytics and insight

Audience

This white paper is intended for customer, partners & prospects who wants to understand how Dell EMC PowerProtect Software helps protecting the VMware workloads.

1 Architecture

Protection Policy

A protection policy allows you to select a specific group of assets that you want to back up. Use the PowerProtect UI to create a virtual machine protection policy.

VM Proxy

The VM proxy (vProxy) protection engine is the virtual machine data protection component within PowerProtect Data Manager. This allows you to deploy a VM proxy in the vSphere environment to perform virtual machine snapshot backups, and then move the backup data to the target storage.

PowerProtect Data Manager Software comes pre-bundled with an embedded VM proxy for environments that do not require concurrent backups and where Hot Add transport mode is not required. For environments that require a large amount of data movement and concurrent data protection operations, Dell EMC recommends deploying an additional external VM proxy for virtual machine backups.

1.1.1 Transport modes:

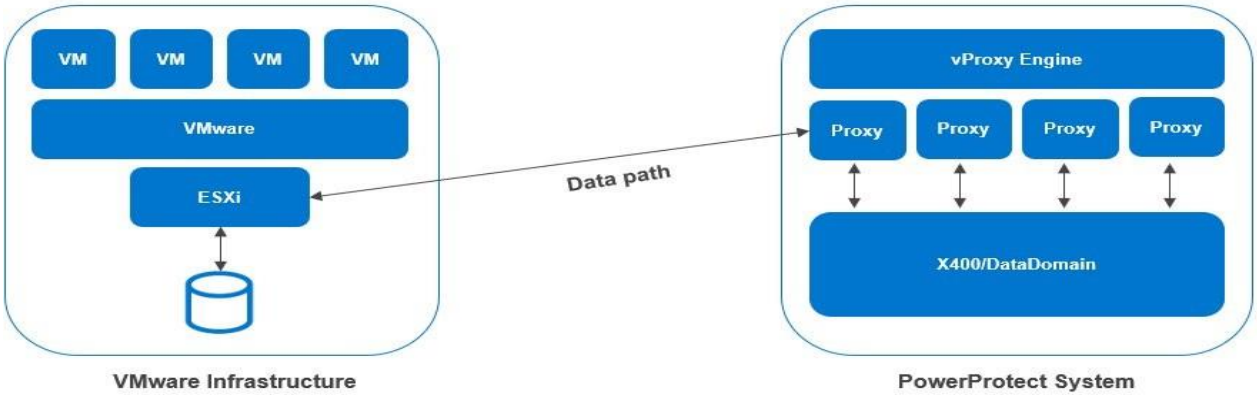
PowerProtect Software support HotAdd and NBD transport modes, the transport mode that you selected when adding the vProxy appliance (Hot-Add, Network Block Device, or the default setting Hot Add, Failback to Network Block Device). In NBD mode, the ESX/ESXi host reads data from storage and sends it across a network to the target storage.

As its name implies, this transport mode is not LAN-free, unlike SAN transport.

HotAdd is a VMware feature where devices can be added “hot” while a virtual machine is running. Besides SCSI disk, virtual machines can add additional CPUs and memory capacity. If backup software runs in a virtual appliance, it can take a snapshot and create a linked clone of the target virtual machine, then attach and read the linked clone’s virtual disks for backup. This involves a SCSI HotAdd on the ESXi host where the target VM and backup proxy are running. Virtual disks of the linked clone are Hot Added to the backup proxy. The target virtual machine continues to run during backup.

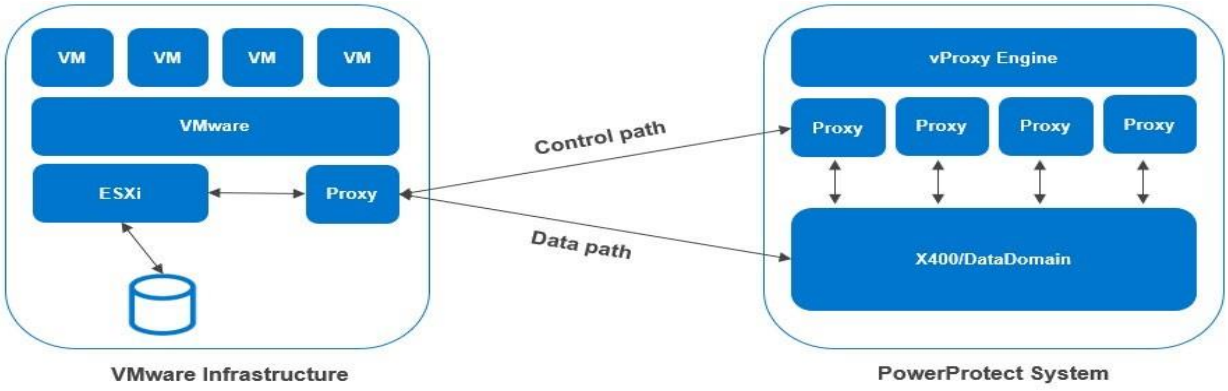
1.1.2 Internal VM proxy engine:

- For small scale environments
- Doesn’t require concurrent backups
- Uses Network Block Device transport mode
- Data is transferred over network to ESX server hosting the proxy
- Proxy gets data from its ESX host and writes to storage

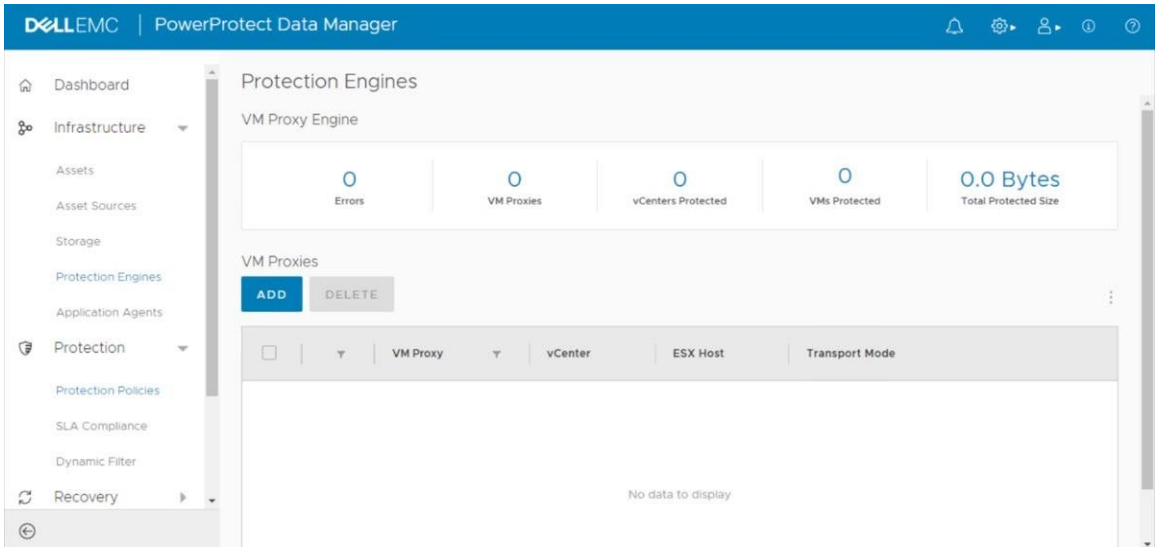


1.1.3 External VM proxy engine

- For larger scale environments
- Requires concurrent data protection operations
- Can also use NDB but preferred method is to use HotAdd transport mode for better performance
- Proxy attaches itself to VM disk snapshot to be backed-up
- Proxy reads data from attached disk and writes to storage



Administrators can navigate to **Infrastructure → Protection Engines** to open the protection engines window to view statistics for the VM proxy engine, manage and monitor VM proxies, and add an external VM proxy to facilitate data movement.



Note: When an additional VM proxy is deployed and registered, this appliance is used by PowerProtect Data Manager instead of the embedded VM proxy. For any data protection operations involving virtual machine protection policies, unless all added VM proxies are unavailable. If no added VM proxy is available, the embedded VM proxy is used to ensure that backups complete successfully

Virtual machine backup: For a virtual machine, you can select from three types

1.1.4 VM consistent backup

- Capture all the virtual machine disks at the same time and back up the data to storage targets to create a transactional-consistent backup
- Use this option for Windows and Linux virtual machines, and for guest operating systems that have applications other than the SQL Server

1.1.5 Application Application-Aware backup

Application aware full backup is an extension of VM full backup. For virtual machines with a SQL application installed, select this type to quiesce the application to perform the SQL database and transaction log backup. When you select this type, you also need to provide Windows account credentials for the virtual machine.

You can provide the credentials at the protection lifecycle (PLC) level and/or the virtual machine asset level. When you provide the credentials at both the PLC level and the virtual machine asset level, the virtual machine asset credentials override the PLC credentials for that virtual machine. These credentials are required because PowerProtect Software interacts with the guest virtual machines to install the Microsoft application agent and quiesce the application for performing application consistent backups.

The agent also enables the application administrator to perform self-service restores by using the native Microsoft SQL Studio Management interface.

Exclusion: Select this type if there are virtual machine assets within the protection policy that you plan to exclude from data protection operations.

2 Deployment Requirements

Network: To protect VMware virtual machine using PowerProtect Software following are the key requirements from network perspective.

Description	Communication	Port
SSH Communication	Bi-directional communication between the SSH	22 TCP
VM proxy agent management	Outbound	9613
VM proxy agent on protected guest VM	Inbound	9613
vCenter Communication	Bi-directional	443

- Ensure PowerProtect Software server time is synchronized with the ESXi host system time. It is critical to PowerProtect operation that the PowerProtect Software server time matches the systems that it interfaces with. Dell EMC recommends that the ESXi host, and all of the systems that the ESXi host interfaces with, be configured to use a NTP server

- Use Fully Qualified Domain Names (FQDNs) where possible

- Ensure that forward and reverse DNS lookups work for each host in the protection

Minimum supported hardware requirements for the ESXi host PowerProtect Software requires a minimum of vSphere 6.0 software version to deploy in VMware environments.

2.1 Requirements for Application Aware backups on virtual machines

- vSphere version 6.5 and later
- VMware ESXi server version 6.5 and later
- VMware Tools version 10.1 and later

Component	Requirements
vCenter server	Version 5.5, 6.0, 6.5, 6.7 Note: Version 6.5 and later is required to perform Microsoft SQL Server application-aware protection.
VMware Tools	Version 10 or later. Note: Version 10.1 and later is required to perform Microsoft SQL Server application-aware protection.

Note: Supported hardware/software platform may get changed in subsequent releases. Please refer Dell EMC online interoperability portal for the latest product information.
https://elabnavigator.emc.com/eln/modernHomeDataProtection

3 vCenter authentication

It is strongly recommended that you set up a separate vCenter user account at the root level of the vCenter that is strictly dedicated for use with PowerProtect Software and the vProxy protection engine. Use of a generic user account such as “Administrator” might make future troubleshooting efforts difficult as it might not be clear which “Administrator” actions are interfacing, or communicating, with PowerProtect Software. Using a separate vCenter user account ensures maximum clarity if It becomes necessary to examine vCenter logs.

Before you can use the vCenter user account with PowerProtect Software, or before you can use the Single Sign-on (SSO) admin user with the vProxy appliance, the user must be an administrator on the vCenter root node. Users who inherit permissions from group roles are not valid.

Note: VMware protection supports ESX 6.0 U2 and above are supported for VMware Protection. By default, PowerProtect Data Manager enforces SSL certificates during communication with vCenter Server. If a certificate appears, click Verify to accept the certificate. It is highly recommended that you do not disable certificate enforcement.

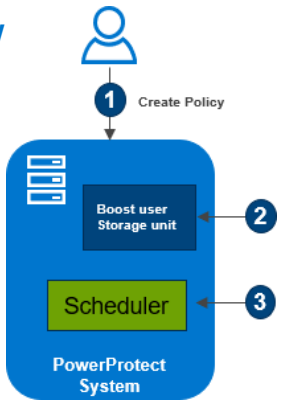
3.1 VADP snapshot

Support Change Block Tracking (CBT) which allows backup applications to determine delta of changes in the VM since last backup and only read and transfer those changes when doing the next backup incrementally PowerProtect Software uses one or more VM proxy for reading VM's disk changes and transferring those.

Any L0 backup of a VM reads the entire contents of all disks and writes the same to storage using DD Boost (leveraging global deduplication), Any non-L0 backup of a CBT enabled VM will only read changes in the disks from last backup and overlay those changes on a copy of last backup to generate a new full backup (while moving only incremental changes).

Backup files are written to storage using fixed size segments (FSS) of 8K. Backup files on storage are always thick, i.e. VMDK file-size on storage is equal to the size of provisioned disk.

4 VM Consistent backup configuration workflow

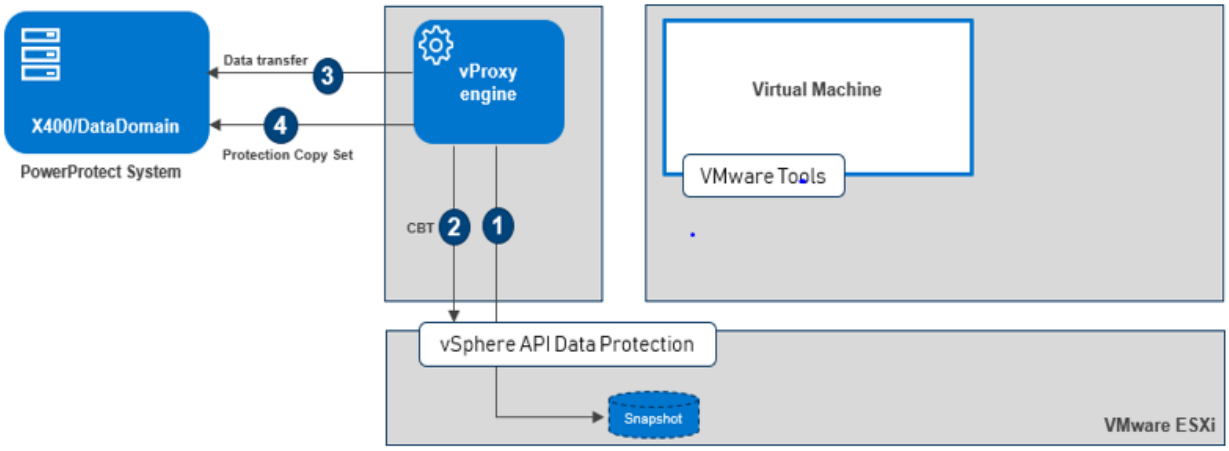


Following is configuration workflow of VM consistent backups

1. User creates protection policy using PowerProtect UI
2. PowerProtect Software creates Boost user and storage-unit on target storage
3. PowerProtect Software adds protection schedule to its own scheduler

4.1 VM consistent backup protection workflow

Following is Protection workflow of VM consistent backups

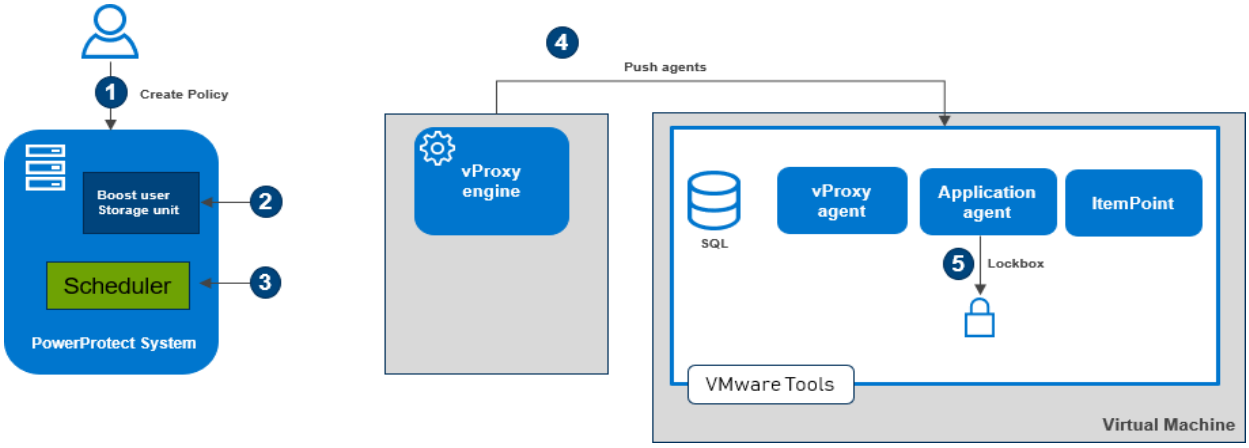


1. VM proxy takes VADP snapshot
2. VM proxy gets changed blocks from VADP
3. VM proxy starts data transfer to target storage
4. PowerProtect Software creates VM PCS (Protection Copy Set) based on the backup results

4.2 Application-aware backup configuration workflow

Following is the configuration workflow of application-aware backups

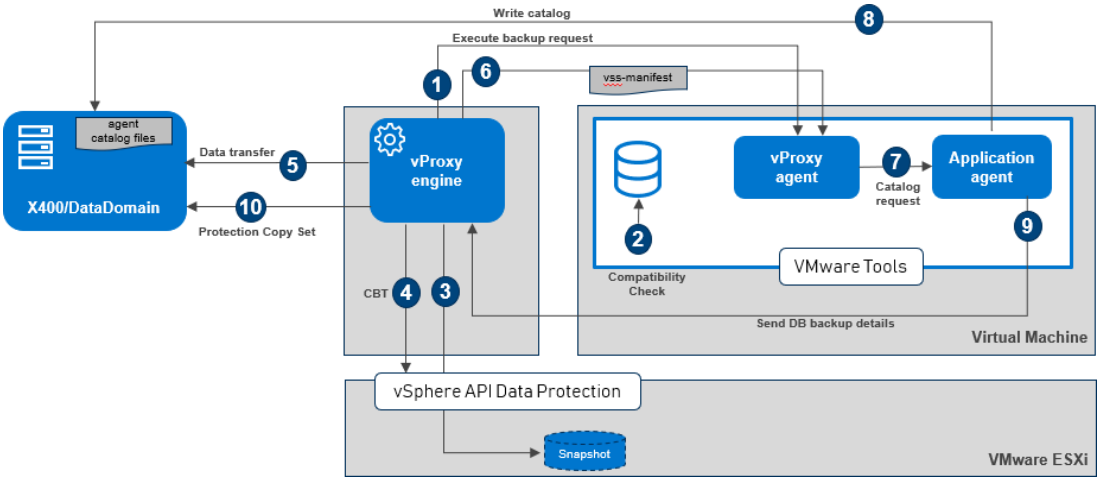
1. User creates protection policy using PowerProtect Data Manager
2. PowerProtect Software creates Boost user and storage-unit on target storage
3. PowerProtect Software adds protection schedule to its own scheduler
4. vProxy engine pushes agent using guest OS credentials
- Microsoft application agent
- Dell EMC vProxy agent
- Dell EMC ItemPoint
5. Application agent configures lockbox with credentials on SQL host (using ADM)



4.3 Application-aware backup protection workflow (FULL)

Following is the protection workflow of application aware DB backups

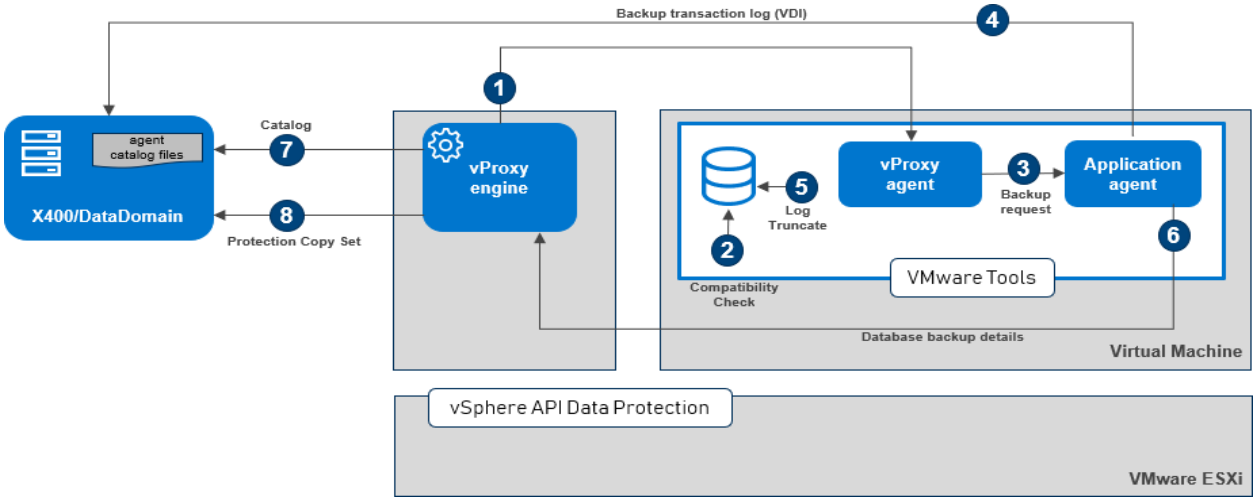
1. Request to vProxy agent to execute backup
2. Application-aware compatibility check (SQL permission, SQL status, VSS status, etc.)
3. vProxy takes VADP snapshot with quiesce option which will internally trigger VMware's own VSS workflow
4. vProxy gets changed blocks from VADP
5. vProxy starts data transfer to target storage
6. vProxy retrieves VSS manifest (metadata) from vSphere using VADP API and uploads it to the guest VM
7. vProxy tells Microsoft app agent to catalog the backup
8. App agent parses VSS manifest and catalogs databases quiesced during step 3 under its own directory structure on storage
9. App agent provides database backup details, including discovered SQL assets, to vProxy
10. PowerProtect Software creates VM PCS (Protection Copy Set) and corresponding SQL PCS based on the backup results



4.4 Application-aware backup workflow (LOG)

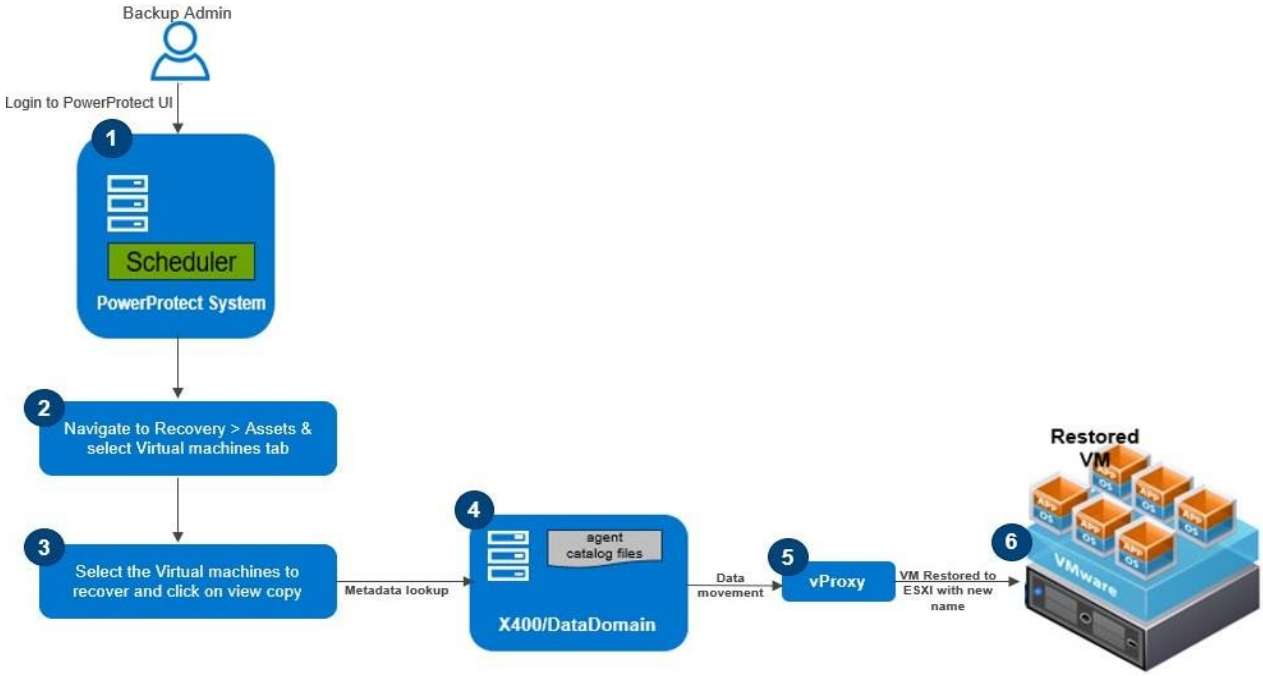
Following is the protection workflow of application aware log backups

1. Request to vProxy to execute backup
2. Application-aware compatibility check (SQL permission, SQL status, VSS status, etc.)
3. vProxy asks Microsoft App agent to execute transaction log backup
4. Microsoft App agent will serially back up each database transaction log (using VDI) directly to target storage
5. SQL Server truncates logs
6. App agent provides database backup details, including discovered SQL assets, to vProxy
7. vProxy parses VSS manifest and catalogs files and transaction logs
8. PowerProtect Software creates VM PCS and its corresponding SQL PCS based on the backup results



5 Dell EMC PowerProtect Software use-cases for virtual machine recovery

Restore to new: Create a new virtual machine using a copy of the original virtual machine backup and can be restored on the vCenter server using a different name. Using restore to new option VM Can also be restored on an alternate vCenter server if it has been discovered by PowerProtect Software previously. Instant access allows the VM to be created and powered on while temporarily accessing the. vmdk from PowerProtect. The virtual machine becomes available for use as soon as it is powered on. Following flow diagram provides the overview of Restore to new recovery operation.



Restore to original: Recover virtual machine backup to its original location on the same vCenter Rollback the virtual machine that was protected to an earlier point in time. Unlike Restore to New, there are no options to be selected. A dialog box will appear, requesting confirmation that you want to restore this virtual machine.

Live virtual machine: Creates a new virtual machine directly from the original virtual machine backup for the purposes of instant backup validation and recovery of individual files. This process does not copy or move any data from storage to the production datastore. VMware administrator can vMotion the VM manually. The live virtual machine is initially available for a period of 7 days. Monitor and manage the live virtual machine recovery from the Instant Access menu.

File level restore: File level restore allows you to recover individual files from backups of virtual machines or VMDKs performed in PowerProtect Data Manager to a primary or secondary vCenter server. File-level restore is only supported for the following platforms and operating system versions.

Note: File level restore is only supported for the following platforms and operating system versions. File level restore in the PowerProtect Data Manager UI can only be performed by an administrator.

- ✓ RedHat Enterprise Linux versions 6.x and 7.x
- ✓ SuSE Linux Enterprise Server versions 11.x and 12.x
- ✓ Debian version 9.1
- ✓ Ubuntu version 17.10
- ✓ CentOS version 7.2
- ✓ Oracle Enterprise Linux version 7.2
- ✓ Windows 7, 8, 10, Server 2008, 2012, 2016 (all 64-bit platforms and R2, where applicable) for FAT, and NTFS

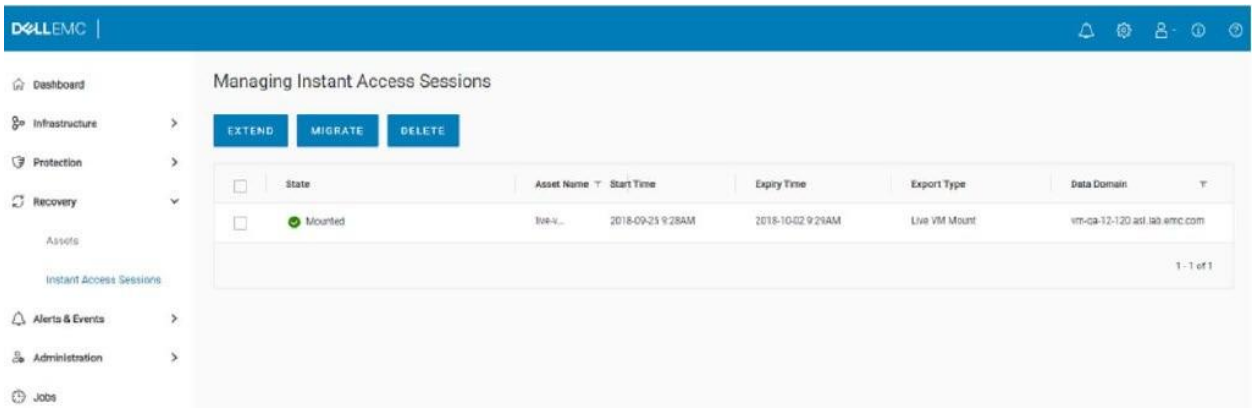
Manage and monitor Instant Access Sessions

The Instant Access Sessions window allows you to manage the status of a virtual machine restore to new or instant access virtual machine restore. For example: By extending the availability period or deleting an instant access virtual machine) and monitor vMotion events.

Note: The Instant Access Sessions used by a SQL application-aware self-service restore are displayed in the PowerProtect Data Manager UI, but management is disabled. Use the SQL application-aware self-service restore UI to manage these sessions.

When the Jobs window indicates that a recovery has completed successfully, go to Restore > Instant Access sessions to access the Managing Instant Access Sessions window. This window allows you to monitor and manage all exported copies that you have created from storage.

An active restore session with a state of Mounting indicates that the restore is still in progress. Once the state changes to Mounted, the restore is complete and the instant access virtual machine is ready. When you select the checkbox next to the session, you can choose from three options, as shown in the following figure



Best Practices with vProxy appliance

Observe the following best practices when using PowerProtect Software with the vProxy appliance

- Install VMware Tools on each virtual machine by using the vSphere Client. VMware Tools adds additional backup and recovery capabilities that quiesce certain processes on the guest operating system prior to backup
- Use HotAdd transport mode for faster backups and restores and less exposure to network routing, firewall, and SSL certificate issues. To support HotAdd mode, deploy the vProxy on an ESXi host that has a path to the storage that holds the target virtual disk(s) for backup
- HotAdd mode requires VMware hardware version 7 or later. Ensure all virtual machines that you want to back up are using virtual machine hardware version 7 or later
- For sites that contain many virtual machines that do not support HotAdd requirements, NBD transport mode will be used

VM Proxy limitations and unsupported features

Following limitations and unsupported features related to the VM Proxy.

VMware limitations by vSphere version: VMware limitations for vSphere 6.0 and later versions are available at https://configmax.vmware.com/home.

For vSphere 5.5, go to https://www.vmware.com/pdf/vsphere5/r55/vsphere-55- configuration-maximums.pdf

VM Proxy configuration settings cannot be modified after adding the VM Proxy: After adding a VM Proxy, the only field you can modify is the Transport Mode. Any other configuration changes require you to delete and then re-add the VM Proxy

Network configuration settings do not get restored with virtual machine after recovery of a vApp backup Network configuration settings are not backed up with the virtual machine as part of a vApp backup. As a result, when you restore a vApp backup, you must manually reconfigure the network settings

VM Proxy configured with dual stack is not supported The VM Proxy does not support dual stack (IPv4 and IPv6) addressing. If you want to run backups and restores using the VM Proxy, use IPv4 only addressing

Virtual machine alert "VM MAC conflict" may appear after successful recovery of virtual machine After performing a successful recovery of a virtual machine through vCenter version 6, an alert may appear indicating a "VM MAC conflict" for the recovered virtual machine, even though the new virtual machine will have a different and unique MAC address. You must manually acknowledge the alert or clear the alert after resolving the MAC address conflict. Note that this alert can be triggered even when the MAC address conflict is resolved.

The VMware release notes at http://pubs.vmware.com/Release_Notes/en/vsphere/60/vsphere-vcenter-server-60u2-release-notes.html provide more information.

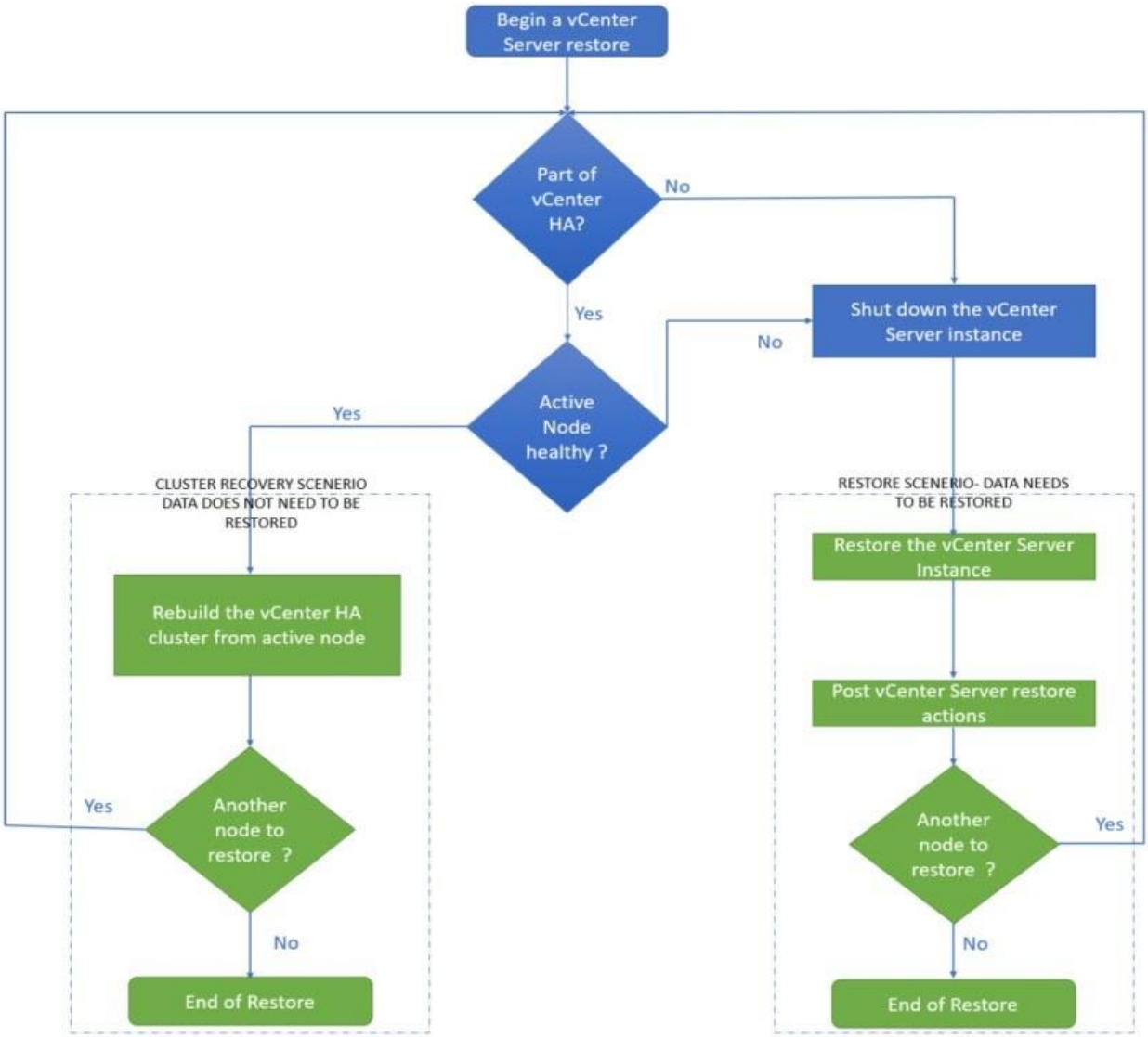
Protection fails for virtual machine name containing { or } PowerProtect Data Manager virtual machine protection policy fails to back up virtual machines that contain the special characters { or } in the name. This limitation exists with vSphere versions previous to 6.7. If you do not have vSphere 6.7 installed, avoid using these two characters in virtual machine names.

Datastore names cannot contain special characters Using special characters in datastore names can cause problems with the VM Proxy, such as failed backups and restores. Special characters include the following: % & * $ # @ ! \ / : * ? " <> | ;, and so on.

HotAdd backups fail when datacenter names contain special characters Virtual machine backups fail when the datacenter name contains special characters and the transport mode specified for VM Proxy backups is Hot Add only. Avoid using special characters in the datacenter name, for example, "Datacenter_#2@3", or specify HotAdd with fallback to Network Block Device for the transport mode.

6 Disaster Recovery

PowerProtect Software supports protecting vCenter 6.5 deployments using vProxy appliance. It will be useful in case disaster or vCenter down scenario to recovery the virtualized environments. Following are the recommendations and best practices when planning a vCenter virtual machine or its component virtual machines backup.



- It is recommended to schedule the backup of the vCenter server when the load on the vCenter server is low, such as during off-hours, to minimize the impact of vCenter virtual machine snapshot creation and snapshot commit processing overhead

- Ensure that there are no underlying storage problems that might result in long stun times
- Keep the vCenter virtual machine and all its component virtual machines in one single isolated

NetWorker group/policy. This is to ensure that the backup times of all vCenter server component virtual machines are as close to each other as possible

- If using one or more external Platform Services Controllers, it is recommended to have one dedicated vProxy associated to the workflow for the entire vCenter server virtual machines backup. This will ensure that the backup times of all vCenter Server component virtual machines are as close to each other as possible

- Set the maximum HotAdd session limit of the dedicated vProxy to an appropriate number to avoid queuing of backups. It is recommended to set the maximum HotAdd session limit to 25 and the maximum NBD session limit to 0 (zero)

- Ensure that the backup start time of the vCenter Server does not overlap with any operations for other protected virtual machines being managed by this vCenter so that there is no impact on other protected virtual machines during snapshot creation and snapshot commit of the vCenter virtual machine
- If the vCenter Server and Platform Services Controller instances fail at the same time, you must first restore the Platform Services Controller and then the vCenter Server instances

Conclusion

Dell EMC launched Next Generation Multi-Dimensional Data Management Appliance with makes the VMware Data Protection and Recovery simple and provides flexibility to customer for both backup and recovery.

References

For additional information, the following resources are recommended:

Product documentation:

PowerProtect_ Data _Manager_Administration_and User_Guide

PowerProtect E-LAB Navigator

Provides compatibility information, including specific software and hardware configurations that PowerProtect supports. To access E-LAB Navigator, go to https://elabnavigator.emc.com/eln/modernHomeDataProtection.