Technical White Paper

Dell EMC PowerProtect Data Manager: Protection for VMware Cloud Foundation on Dell EMC VxRail

Image-based backup and recovery

Abstract

VMware® Cloud Foundation (VCF) on Dell EMC™ VxRail™ provides the path to hyperconverged infrastructure. This document describes the integration of Dell EMC PowerProtect Data Manager software with VxRail and how VCF workloads on VxRail are protected.

July 2020

H18406

Revisions

Date	Description
July 2020	Initial release

Acknowledgments

Author: Abhishek Shukla, Solutions Technical Marketing Team, Data Protection Domain

Table of contents

Executive summary

Enterprises worldwide are using virtualized platforms to improve IT efficiency and performance, but the need for fast-growing infrastructure presents new challenges. IT organizations must virtualize the rest of the data center, making all infrastructure services become as inexpensive and easy to provision and manage as virtual machines. The solution to address this challenge is the software-defined data center (SDDC): the ideal architecture for private, public, and hybrid clouds.

The VMware vision of the modern data center is a software-defined, standardized architecture. It is a fully integrated hardware and software stack that is simple to manage, monitor, and operate. The VMware architecture for SDDC empowers organizations to run hybrid clouds and incorporate unique capabilities to deliver key outcomes that enable efficiency, agility, and security. The VMware SDDC is based on VMware® vSphere®, VMware vSAN™, and VMware NSX® to provide compute, storage, and networking virtualization to the SDDC. The VMware vRealize Suite® is included in the SDDC for additional cloud management, self-service, automation, intelligent operations, and financial transparency.

Dell Technologies™ shares the VMware vision of the modern data center and extends that to the infrastructure. For customers that choose VMware as the primary technology for modernizing their data center or building a multicloud IT environment, Dell Technologies offers both automated and guided paths to the VMware SDDC. VMware Cloud Foundation™ (VCF) on Dell EMC VxRail™ is a unique, differentiated solution from Dell Technologies.

Dell EMC PowerProtect Data Manager enables users to protect, manage, and recover data in on-premises, virtualized, and cloud deployments. This platform provides centralized governance that helps mitigate risk and assures compliance of SLAs and SLOs through simple protection workflows. It enables automated discovery and onboarding of databases, VMs, and PowerProtect Data Domain as protection storage, and allows self-service and centralized protection for Microsoft® SQL Server® and Oracle® databases. PowerProtect Data Manager covers many cloud data-protection use cases, such as long-term retention, cloud disaster recovery, backup to cloud, and in-cloud backup. It also includes a SaaS-based reporting solution for management, compliance, and predictive analytics.

Audience

This white paper is intended for customers, partners, and others who want to understand how PowerProtect Data Manager Software helps protect VCF workloads on VxRail.

Scope

The scope of this white paper is limited Dell EMC PowerProtect Data Manager (software) protecting VCF workloads on VxRail. It also describes how to perform image-level backup and recovery of VCF workloads on VxRail.

The components and versions used in this document include the following:

- PowerProtect Data Manager 19.3
- VMware Cloud Foundation (VCF) 3.9
- Dell EMC VxRail 4.7

1 Introduction

Data owners, IT administrators, and developers in midsized or enterprise organizations seek a consistent software platform to simplify management, capacity growth, development, deployment, and upgrades. As businesses consume IT resources differently, there is a need for powerful, efficient, and trusted data protection, enabling organizations to transform and meet future demands when modernizing their IT environment. VMware Cloud Foundation (VCF) on Dell EMC VxRail, combined with Dell EMC PowerProtect Data Manager to protect workloads, is one solution to these modern challenges.

VMware Cloud Foundation provides integrated cloud infrastructure (vSphere compute, vSAN storage, NSX networking, and security) and cloud management services (with the vRealize Suite) to run many types of enterprise applications. This can range from traditional applications, deployed as virtual machines and VMware Horizon virtual desktops, to Kubernetes powered containerized cloud-native applications, and can include private and public environments. Dell EMC PowerProtect Data Manager is an effective solution to protect these environments.

1.1 VMware Cloud Foundation on VxRail

VMware Cloud Foundation on VxRail provides the simplest path to the hybrid cloud. By deploying Cloud Foundation on VxRail, customers get full-stack integration with both the HCI infrastructure layer and VMware cloud software stack. Automated life-cycle management is provided as a single, complete, turnkey hybrid cloud experience, greatly reducing risk and increasing IT operational efficiency.

1.1.1 VxRail Manager

The VxRail HCI System Software includes a suite of leading-edge capabilities for VxRail that offer a highly differentiated experience. The most-used and most familiar feature of the VxRail HCI System Software is the VxRail Manager (available now as a vCenter plug-in), which is the primary deployment and element manager for VxRail.

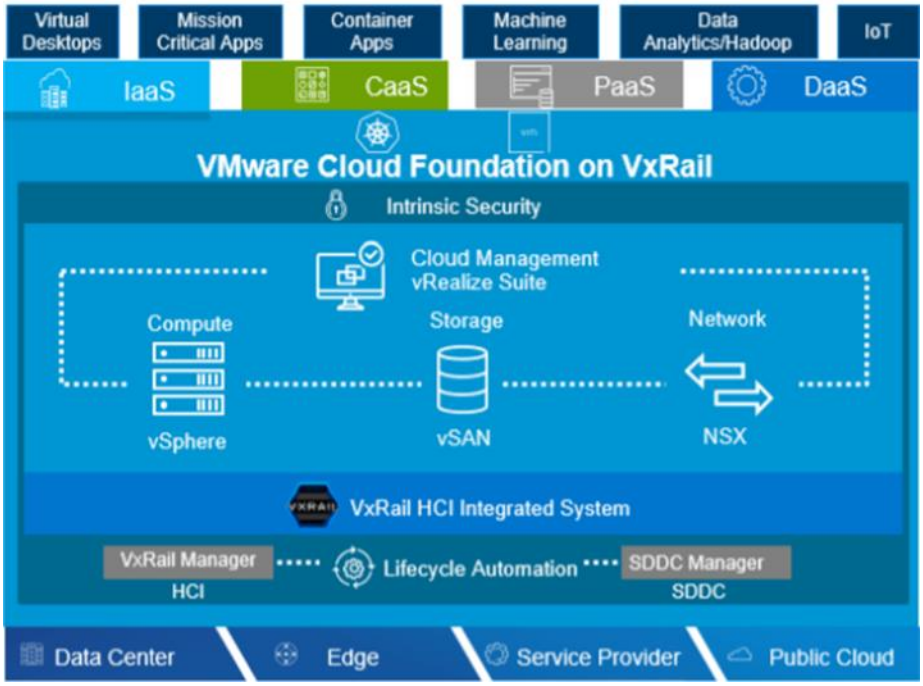


Figure 1 VMware Cloud Foundation on VxRail

VCF on VxRail uses VxRail Manager to deploy and configure vSphere clusters that are powered by vSAN. It is also used to run the Lifecycle Manager (LCM) of VMware ESXi™, vSAN, and firmware using a fully integrated and seamless process that is orchestrated by SDDC Manager. It monitors the health of hardware components and provides remote service support.

1.1.2 SDDC Manager

SDDC Manager orchestrates the deployment, configuration, and LCM of vCenter, and NSX that is above the ESXi and vSAN layers of VxRail. It unifies multiple VxRail clusters as a workload domain (WLD) or as multiple WLDs. For multiple-availability zones (multi-AZs), SDDC Manager creates the stretched cluster configuration for a dual-availability zone (AZ) WLD.

1.1.3 Network virtualization

VMware NSX Data Center is the network virtualization and security platform that enables the virtual cloud network. It is a software-defined approach to networking that extends across data centers, clouds, endpoints, and edge locations. With NSX Data Center, network functions—including switching, routing, firewalling, and load balancing—are brought closer to the application and distributed across the environment. Similar to the operational model of virtual machines, networks can be provisioned and managed independent of underlying hardware. NSX Data Center reproduces the entire network model in software, enabling any network topology—from simple to complex multitier networks—to be created and provisioned in seconds. Users can create multiple virtual networks with diverse requirements, leveraging a combination of services that are offered by NSX. You can build more agile and secure environments with services that include micro-segmentation and third-party integrations from a broad ecosystem, ranging from next-generation firewalls to performance-management solutions. These services can be extended to several endpoints within and across clouds.

1.1.4 vRealize Suite

Part of the vRealize Suite, vRealize Automation provides enhanced support to NSX to implement network automation, and vRealize Operations allow centralized capabilities for performance, capacity configuration, and compliance management. vRealize Log Insight provides heterogeneous and highly scalable log management with intuitive, actionable dashboards, sophisticated analytics, and broad third-party extensibility, providing deep operational visibility and faster troubleshooting.

1.1.5 Cloud management

The cloud management platform (CMP) is the main consumption portal for the SDDC. You can use vRealize Automation to author, administer, and consume VM templates and blueprints. As an integral component of VCF, vRealize Automation provides a unified service catalog that gives IT or users the ability to select and run requests to instantiate specific services.

1.2 Workload domain architecture

Within the workload domain architecture (WLD), the domain starts with a single VxRail cluster. The cluster can have a minimum of three VxRail hosts in each VxRail cluster, and it scale up to maximum configurations supported by vSphere or VSAN. Multiple clusters can be created per domain. Each domain has its own vCenter server instance and is patched and upgraded independently. The vCenter Server instance for all the workload domains is configured with enhanced linked mode. This mode allows for a central visibility and control while also allowing role-based access controls to be used to secure and limit access. Multicluster domains enable scalability.

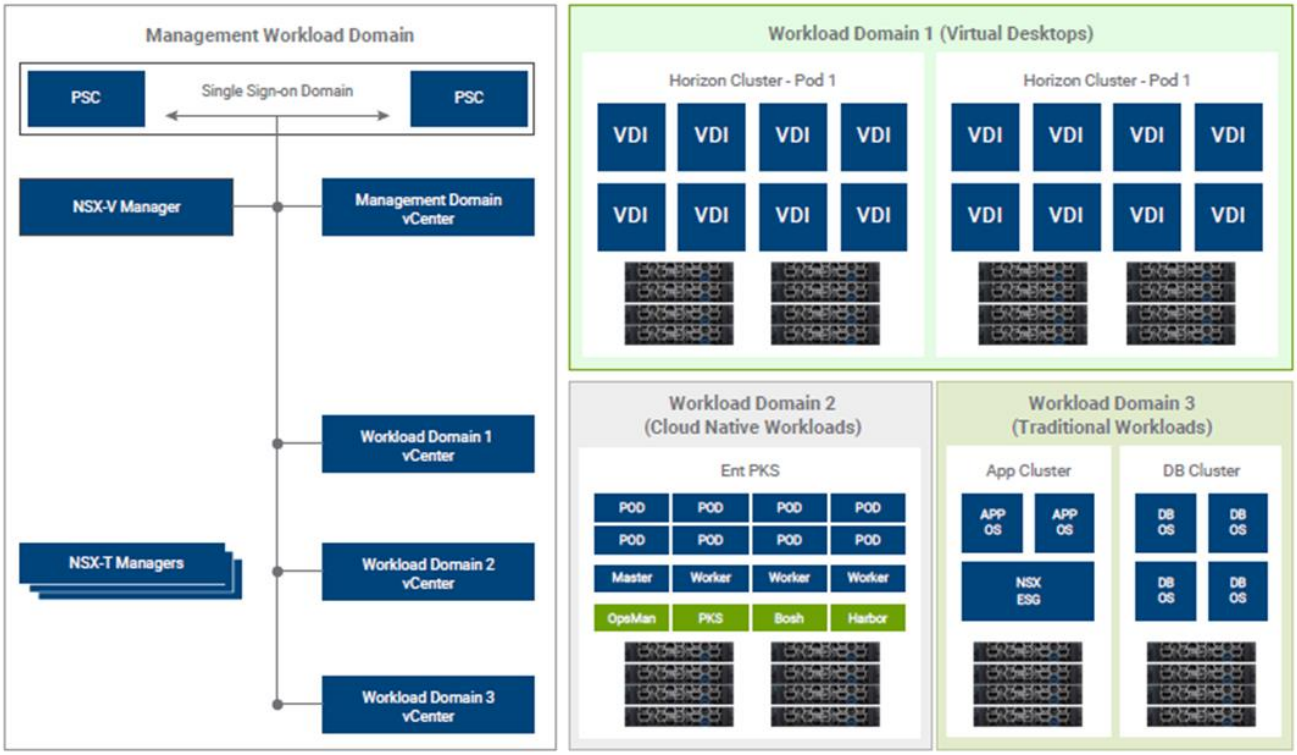


Figure 2 Workload domain architecture

From the VxRail clusters, you can organize separate pools of capacity into WLDs, each with its own set of specified CPU, memory, and storage requirements. These WLDs can support various workloads types such as VMware Horizon® or business-critical apps like databases.

Two types of WLDs can be deployed:

- Management WLD (Mgmt WLD) with single per-VCF instance
- Virtual Infrastructure (VI) WLD

1.2.1 Management workload domain

The management workload domain (Mgmt WLD) cluster requires a minimum of four hosts that run the infrastructure components used to instantiate and manage the private cloud infrastructure. For VCF on VxRail, the management WLD should not be used to host business workloads. This management WLD is created during initial system installation (or bring-up) using the VCF Cloud Builder tool.

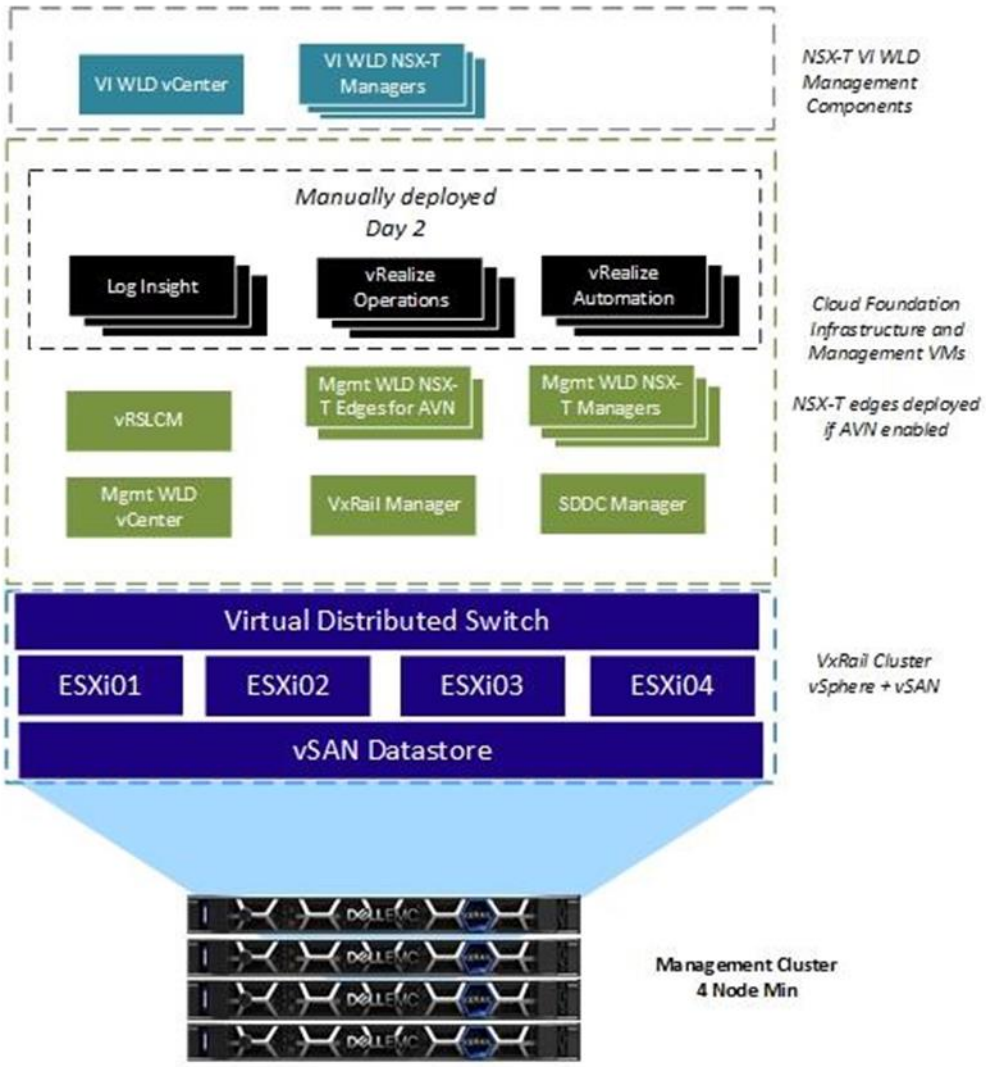


Figure 3 Management WLD cluster

In the Management WLD cluster, vSphere runs with a dedicated vCenter server that is backed by vSAN storage. It hosts SDDC Manager and VxRail Manager VMs, NSX-V, and vRealize Log Insight for management domain logging. Other components such as vRealize Operations and vRealize Automation are optional. If a Horizon WLD is deployed, the management components are also deployed in the Mgmt WLD. The management cluster must have a minimum of four hosts to provide vSAN FTT=1 during maintenance operations. While the deployment and configuration of the management cluster is fully automated when it is running, it can be managed like the other VxRail cluster by using the vSphere HTML5 client.

1.2.2 vCenter Server design

The management domain vCenter Server is deployed using the standard VxRail cluster deployment process that uses internal VCSA deployment. This vCenter Server is configured as an external vCenter using the vCenter server UI.

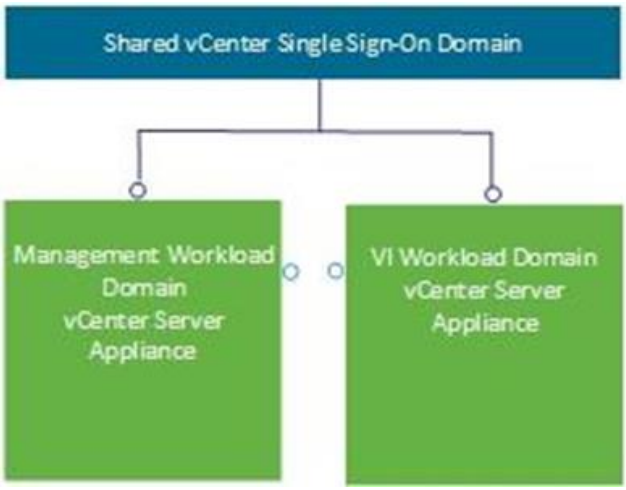


Figure 4 vCenter Server domain

This conversion is performed for two reasons:

- It establishes a common identity management system that can be linked between vCenter servers
- It allows the SDDC Manager LCM process to manage the life cycle of all vCenter components in the solution

1.2.3 Virtual infrastructure workload domain

The virtual infrastructure workload domain (VI WLD) can consist of one or more VxRail clusters. The VxRail cluster is the building block for the VxRail VI WLD. The first cluster of each VI WLD must have four hosts, but subsequent clusters can start with three hosts. The VI WLD can be either an NSX-V based WLD or an NSX-T based WLD. This can be selected when adding the first cluster to the WLD. The vCenter and NSX-V or NSX-T Manager for each VI WLD are deployed into the Mgmt WLD. For an NSX-V based VI WLD, the controllers are deployed to the first cluster in the VI WLD that is added by the SDDC Manager. Each new VI WLD requires an NSX-V Manager to be deployed in the Mgmt WLD and the three controllers deployed into the first cluster of the VI WLD.

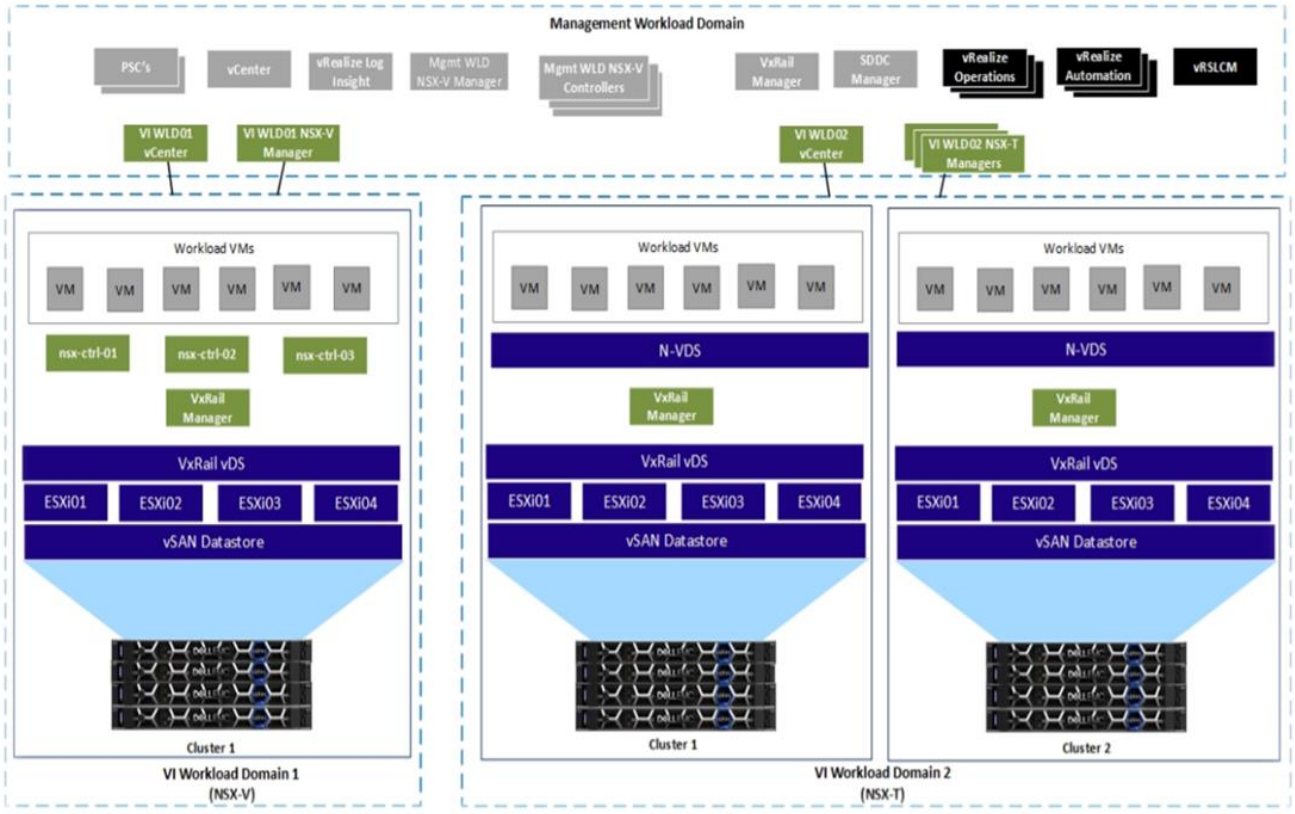


Figure 5 Virtual infrastructure workload domains

For an NSX-T based VI WLD, when the first cluster is added to the first VI WLD, the NSX-T Managers (three per cluster) are deployed to the Mgmt WLD. Subsequent NSX-T based VI WLDs do not require additional NSX-T mangers, but each VI WLD VI is added as a compute manager to NSX-T.

For both NSX-T based VI WLDs and NSV-V based VI WLDs, the first cluster can be considered a compute- and edge cluster since it contains both NSX and compute components. NSX virtual routers can be deployed to this first cluster. The second and subsequent clusters in a VI WLD can be considered compute-only clusters since they do not host any NSX routing virtual machines.

1.2.4 VCenter Server design

The VI WLD vCenter server is deployed by the SDDC Manager when creating a VI WLD. It is deployed in the Mgmt WLD. During deployment, it is added to the existing SSO domain, allowing a single pane of glass to manage both the management and VI WLD vCenter servers.

1.3 PowerProtect Data Manager

PowerProtect Data Manager provides software-defined data protection, deduplication, operational agility, self-service and IT governance for physical, virtual, and cloud-based environments. This platform provides centralized governance that helps mitigate risk and assures compliance of SLAs and SLOs through simple protection workflows. It enables automated discovery and onboarding of databases, VMs, integrated storage, self-service, and centralized protection for databases and containers. It also includes a SaaS-based reporting solution for management.

PowerProtect Data Manager capabilities include the following:

- Is a software-defined stand-alone solution that is deployed as an open virtual appliance (OVA) in the vCenter environment. It runs as a virtual machine and stores backups to connected integrated storage.
- Discovers workloads such as virtual machines, databases (SQL, Oracle, SAP HANA and Exchange), file systems, and Kubernetes, and protects its assets by creating policies.
- Protects and manages the workloads based on the protection life cycle (PLC).

PowerProtect Data Manager protects workloads of VCF on Dell EMC VxRail. The workloads have respective vCenter Servers which are discovered as an **asset source** once registered with PowerProtect Data Manager. It then discovers the associated assets (VMs) and creates policies for scheduled backup with PLC.

1.3.1 VM proxy (vProxy)

The VM proxy (vProxy) protection engine is the virtual machine data protection component within PowerProtect Data Manager. During backups, the vProxy agent creates a snapshot of virtual-machine data directly from the datastore. The snapshot is moved directly to the target storage where the backups are stored. This process uses VMware vSphere Storage API for Data Protection (VADP) which enables centralized, off-host, LAN-free backup of VCF virtual machines.

The VADP is a subset of the vSphere API that enables backup and restore applications. The snapshot-based VADP framework allows efficient, off-host, centralized backup of virtual-machine storage. After taking a snapshot to quiesce virtual disks, software can offload the backup load to the target storage.

1.3.1.1 Transport modes

PowerProtect Data Manager supports HotAdd and NBD transport modes, which are the transport modes that you select when adding the vProxy appliance (HotAdd, Network Block Device, or the default setting of HotAdd, Failback to Network Block Device).

In NBD mode, the ESX™ or 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 that enables devices to be hot-added 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, and 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.

1.3.2 Protection life cycle

The protection life cycle (PLC) provides central scheduling and manages timing of launching replication jobs per asset. If replication has been configured as a scheduled job, PLC processes the PLC group within the replication window, calling into the replication manager service. If the replication objective does not have a predefined time window, PLC waits for the copy-creation event (successful copy creation) and calls it into the replication manager service. PLC invokes the managed file replication service.

2 Architecture

PowerProtect Data Manager software is a virtual appliance that is deployed on an ESXi host using OVA. PowerProtect Data Manager is integrated with PowerProtect Data Domain Virtual Edition as the protection target where the backups are stored.

The SDDC manager is responsible for performing administration tasks on VCF. It deploys vCenter Servers according to the need of workloads, such as for the management workload (Mgmt WLD), and if required, for the virtual infrastructure workload (VI WLD). The management workloads contain management virtual machines: SDDC Manager, NSX manager, vRealize Automation appliances, vRealize Log Insight Node, and vRealize Proxy agents.

The vCenter Servers are registered with the PowerProtect Data Manager using FQDN/IP. PowerProtect Data Manager discovers the management workloads and VI workloads as virtual-machine workloads associated to the vCenter as assets. A protection policy enables selecting a specific group of assets that must be backed up. A virtual machine protection policy (PLC) can be created using the PowerProtect Data Manager UI. PowerProtect Data Manager enables users to protect, manage, and recover data on premises. PowerProtect Data Manager software uses Dell EMC Data Domain™ Virtual Edition (DDVE) for protection storage.

Figure 6 and the steps that follow describe the PowerProtect Data Manager architecture.

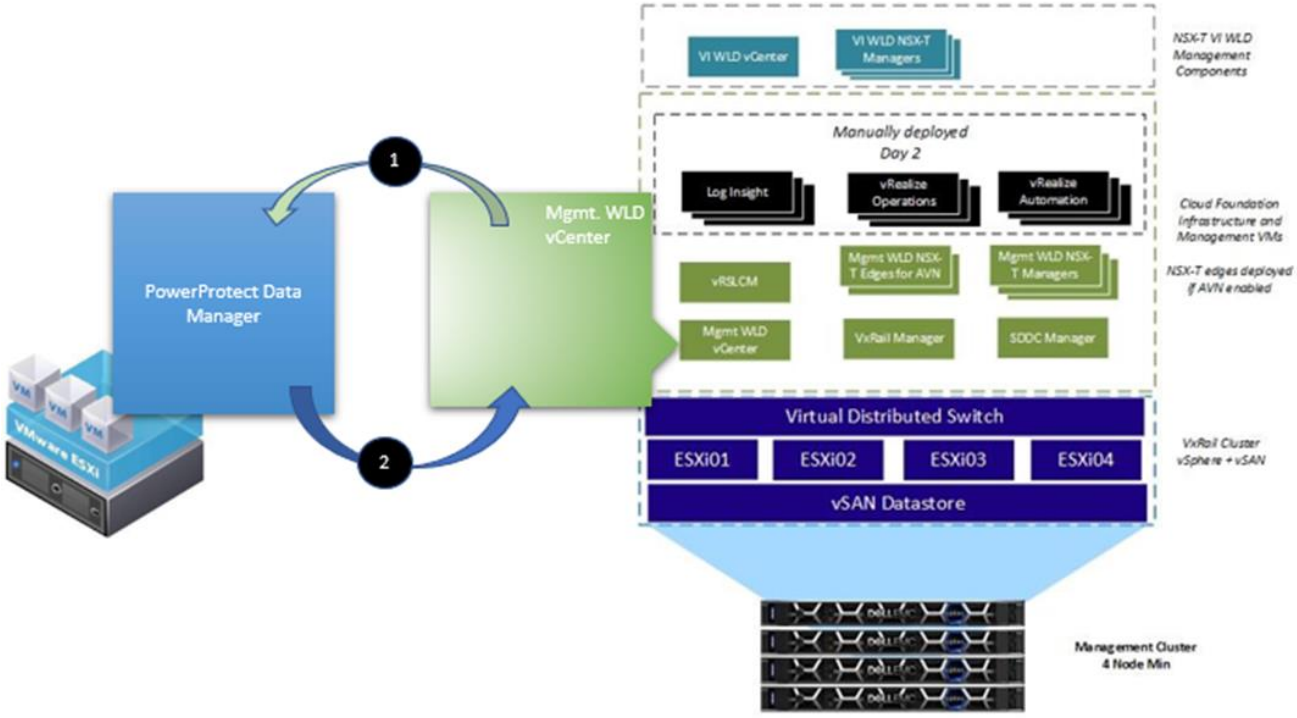


Figure 6 PowerProtect Data Manager architecture

1. The management WLD vCenter is registered with PowerProtect Data Manager.
2. The external VM proxy (vProxy) is installed on the management WLD vCenter server.

Note: Other vProxies are installed with increasing workloads to load balance. A vProxy is created on a load-basis on PowerProtect Data Manager. The number of vProxies depends on the workload on PowerProtect Data Manager.

PowerProtect Data Manager creates the external vProxy and pushes it to vCenter Server where it resides on the ESXi host. PowerProtect Data Manager informs vCenter Server to perform a snapshot for the VM, and the vCenter communicates with the ESXi host to perform a snapshot for the VM. Once the snapshots are taken, it creates differential disk. The vProxy protection engine gets the changed blocks from VADP. The virtual flat disk (vmdk) becomes read-only and is mounted on the vProxy VM which is then pushed to the target storage as a backed-up disk. Once the backup process is completed, the snapshots are consolidated, vProxy removes the mounted disk, it is ready for the next backup.

Figure 7 and the steps that follow describe the protection workflow of VM-consistent backups.

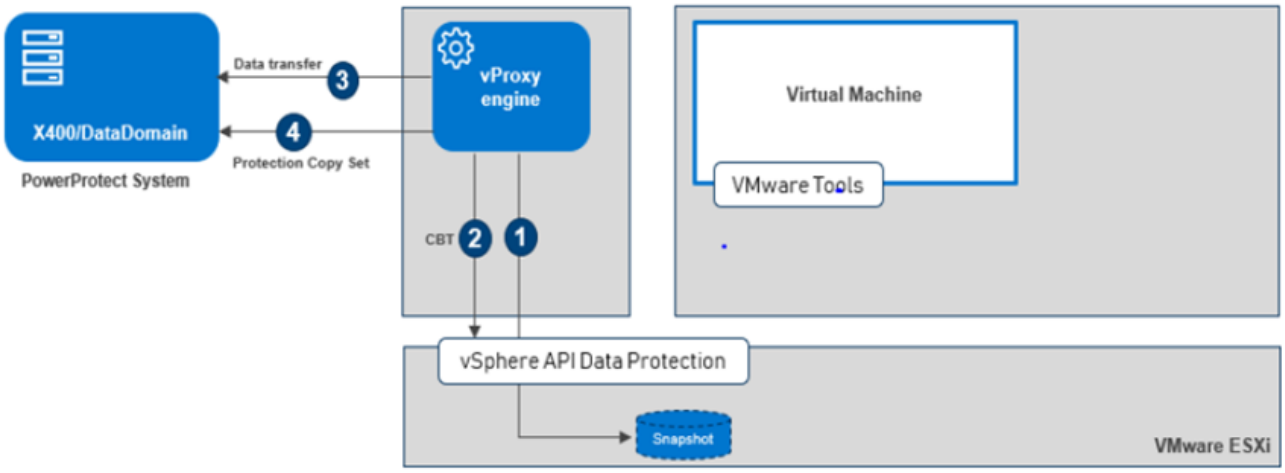


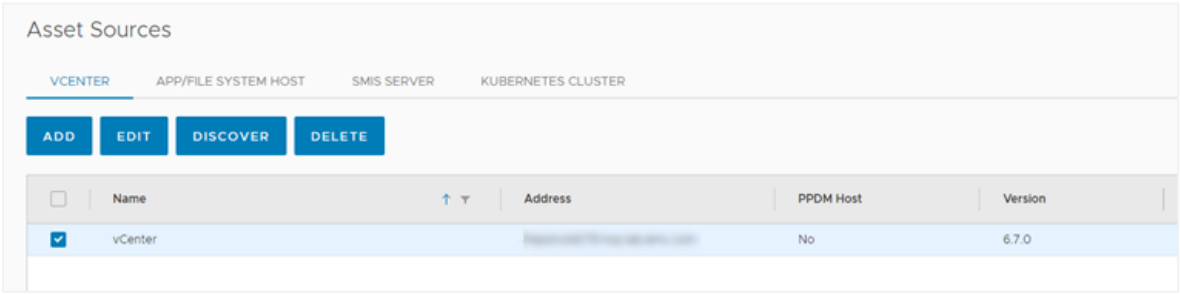
Figure 7 VM-consistent backups

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

2.1 Registering VCF vCenter Server with PowerProtect Data Manager

Perform the following steps to register the VCF vCenter Server with PowerProtect Data Manager:

1. Log in to PowerProtect Data Manager with administrator credentials.
2. On the left pane of the PowerProtect Data Manager UI, click **Infrastructure**.
3. Select **Asset Sources,** and at the top select **VCENTER**.



4. Click **ADD** and enter the following:

- Name of the vCenter server
- FQDN/IP of the vCenter server
- Port: 443
- Enter the host credentials (drop-down menu)
  - VCENTER (default)
  - Name
  - Username
  - Password

5. Click **SAVE.**
6. Check **Schedule Discovery**.
7. Click **SAVE**.

Note: For manual discovery, select the vCenter Server from the list and initiate discovery by clicking **DISCOVER**.

Once the discovery is completed, you can see the virtual machines that are associated to the vCenter Server. These steps would be repeated for the VCF Mgmt WLD and VI WLD vCenter server.

8. On the left pane, slick **Infrastructure** and select **Assets.**

2.2 Backup method

For management workloads, Table 1 shows the core components and the backup methods used.

Table 1 VM core components and backup methods

VM name (core component)	Backup Method
Management vCenter server	Image level
Platform Service Controller	Image level
Management Workload vCenter server	Image level
SDDC manager	Image level
Log Insite Nodes	Image level
NSX-V Manager	File level
NSX-T Manager	File level
VxRail Manager	File level

See the following additional notes:

- NSX-V backup configuration files are scheduled to be backed up to the External FTP Server. Configuration should be done from SDDC Manager console.
- NSX-T backup configuration files are scheduled to backed up to the External FTP. Configuration should be done from NSX-T Manager console.
- To configure automatic backups for VxRail Manager, VxRail Manager performs the backup job to the Management Cluster VSAN datastore.

For information about for file-level backup of NSX components to external FTP, see the VMware document Configure an External SFTP Server for NSX Manager Backups.

Table 2 VM optional components and backup methods

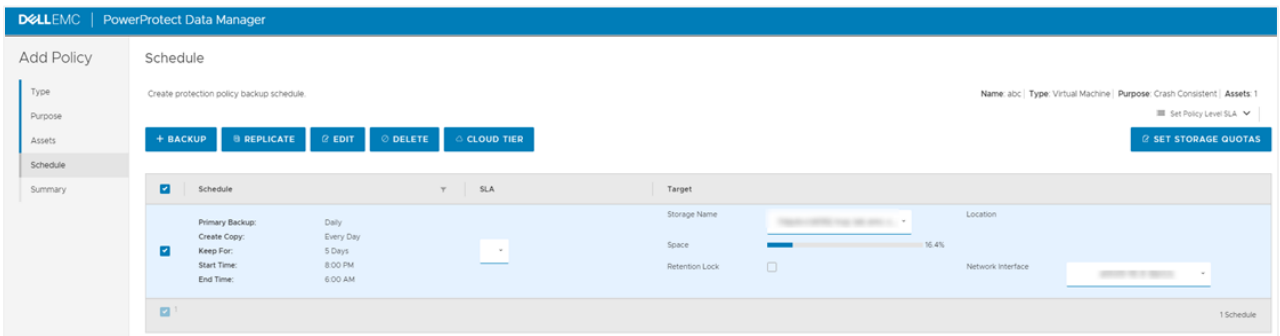
VM name (optional)	Backup method
vRealize Automation Appliances	Image level
vRealize Automation Proxy Agents	Image level
vRealize LogInsight Appliance	Image level
Lifecycle Manager Appliance (LCM)	Image level
Windows SQL Server	Image level or application level

Note: Microsoft SQL VM Backup that is used in this procedure is tested using a VMware image backup for a real production environment. We recommend backing up SQL Server using the application-aware backup method.

2.3 Steps to create backup policy

Use the following steps to create a backup policy:

1. Log in to PowerProtect Data Manager using administrator credentials.
2. On the left pane of the PowerProtect Data Manager UI, click **Protection**.
3. Select **Protection Policies** and click **ADD.**
4. Assign a **Name** to the policy (for example: Test), and add a valid **Description.**
5. For **Type,** select **Virtual Machine** and click **NEXT.**
6. Select the purpose of the policy.
7. Select **Crash Consistent** and click **NEXT.**
8. Select the VM or VMs which need to be protected and click **NEXT.**
9. Click **BACKUP** and schedule the backup per your requirements:
   - You can set up hourly, daily, weekly, or monthly backups
   - Check **Create Full** if you want to take a full backup of the VM, and select the duration per your requirements.
10. **Click OK** to create the backup policy.



Note: There are options to Replicate, Edit, and Delete the selected backup policy. Also, cloud tiering is available, but schedules must have weekly or monthly recurrence and have a retention time of 14 days or greater. Data Domain cloud storage units must be preconfigured on the Data Domain system.

Also, there is an option to set a backup service level agreement (SLA) for the backup policy. You can create this by clicking SLA and using the drop-down menu to choose from the following options:

- Recovery Point Objective (RPO)
- Compliance window
- Verification if the copies are deleted
- Retention Time Objective

To set the backup SLA, click **NEXT**, review the summary, and click **FINISH.**

2.4 Restore plan

The backed-up VMs can be restored any time using a manual process. The backed-up VMs are visible under the recovery tab in PowerProtect Data Manager.

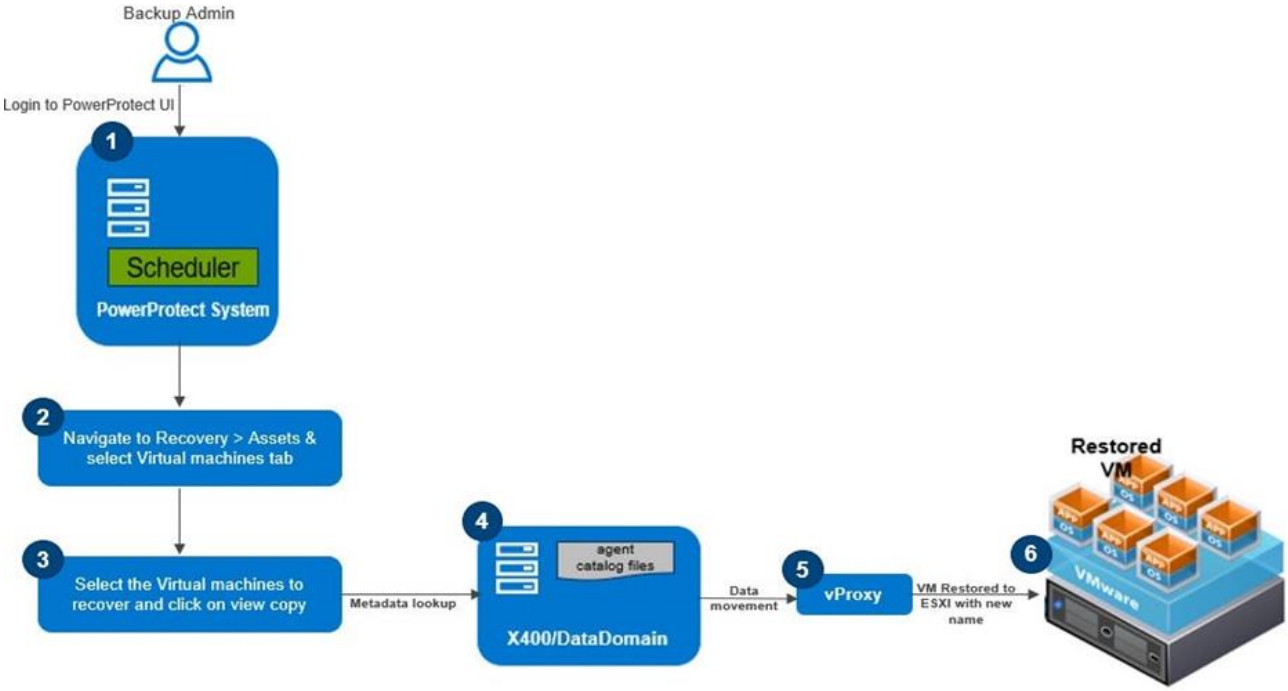


Figure 8 Restore plan

2.4.1 Restore to new

With the **restore to new** option, a new virtual machine is created using a copy of the original virtual machine backup and can be restored on the vCenter Server using a different name. Using the restore to new option, a VM can also be restored on an alternate vCenter Server if it has been discovered by PowerProtect Data Manager 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 when it is powered on. You must wait until each VM is powered on and all its services are started before powering on the next VM.

Note: After a restore, follow the power-on sequence in the VMware Cloud Foundation Operations and Administration Guide.

Table 3 and Table 4 state the restore methods taken for management workload domain.

Table 3 Restore methods

VM name (core components)	Restore method
Management vCenter Server	Image level
Platform Service Controller	Image level
VI Workload Domain vCenter Server	Image level
SDDC Manager	Image level
vRealize LogInsight Node	Image level
DHCP server for NSX	Image level
NSX-V Manager	Deploy OVA, restore the configuration from FTP
NSX-T Manager	Deploy OVA, restore the configuration from FTP
VxRail Manager	Deploy OVA, restore the configuration from FTP

Table 4 Restore methods

VM Name (Optional Components)	Restore Method
vRealize Automation Appliances	Image Level
vRealize Automation Proxy Agents	Image Level
vRealize LogInsight Appliance	Image level
Lifecycle Manager Appliance (LCM)	Image level
Windows SQL Server	Image level

2.4.2 Restore process

Use the following steps to perform a restore:

1. Log in to PowerProtect Data Manager using administrator credentials.
2. On the left pane of the PowerProtect Data Manager UI, click **Recovery**.
3. Select **Assets,** and select the VM or VMs to restore.
4. Click **Restore.**
5. Select the VM name from the list and click **NEXT** (you can select the specific copy of the VM by selecting **CHOOSE COPY**).
6. For the **Purpose**, select **Restore Entire VM** and click **NEXT.**
7. For **Restore Type**, select **Create and Restore to New VM** and click **NEXT.**
8. To choose the VM information (vCenter), use the drop-down menu to select the respective data centers and click **NEXT.**
9. Expand the data center, select the destination host, and click **NEXT.**
10. Expand the storage, select the destination storage for the virtual machine migration, and click **NEXT.**
11. Enter a **New VM Name.**

12. Disable instant VM access for the virtual machine recovery.
13. Check the option for this recovery **Power on the virtual machine when the recovery completes,** and click **NEXT.**
14. Verify the summary and click **RESTORE.**

A Technical support and resources

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

Storage technical documents and videos provide expertise that helps to ensure customer success on Dell EMC storage platforms.

A.1 Related resources

- Dell EMC PowerProtect Data Manager Data Sheet: https://www.dellemc.com/en-me/collaterals/unauth/data-sheets/products/data-protection/h17691-dellemc-powerprotect-software-ds.pdf
- Dell EMC PowerProtect Data Manager: https://www.delltechnologies.com/en-in/data-protection/powerprotect-data-manager.htm#scroll=off
- VCF on Dell EMC VxRail Release Notes: https://docs.vmware.com/en/VMware-Cloud-Foundation/3.9.1/rn/vmware-cloud-foundation-on-dell-emc-vxrail-16-release-notes.html
- VCF Documentation: https://docs.vmware.com/en/VMware-Cloud-Foundation/index.html
- VCF on Dell EMC VxRail architecture: https://www.dellemc.com/resources/en-us/asset/technical-guides-support-information/products/converged-infrastructure/vmware_cloud_foundation_on_vxrail_architecture_guide.pdf