Dell PowerProtect Data Manager: Deployment Best Practices

December 2022

H18564.4

White Paper

Abstract

This white paper explains PowerProtect Data Manager deployment best practices and includes deployment and setup requirements for a new PowerProtect Data Manager.

Dell Technologies

Copyright

Contents

Executive summary

Overview

Data protection has become an integral and essential part of any successful business. The need to provide a powerful, scalable, and simple disaster and operational recovery solution is at an all-time high. IT teams are also looking for a solution that is scalable, easy to implement, efficient to use and handles the workload of their small and medium size environments. To meet midmarket industry demands, Dell Technologies offers Dell PowerProtect Data Manager.

PowerProtect Data Manager enables the transformation from traditional, centralized protection to a Software-as-a-Service (SaaS) model based on a self-service design. This design ensures that you can enforce compliance and other business rules even when backup responsibilities are decentralized to individual database or application administrators.

Some key differentiators for Data Manager are:

- Software-defined backup appliance with integrated deduplication for data protection, replication, and reuse
- Self-service for data owners concerned with central IT governance
- SaaS-based management, compliance, and predictive analytics
- Multidimensional with scale-up and scale-out flexibility and all flash performance
- Microservices architecture for ease of deployment, scaling and upgrading
- Multicloud that is optimized with integrated cloud tiering and cloud disaster recovery

This paper focuses on the PowerProtect Data Manager deployment requirements and best practices.

Audience

This white paper is intended for customers, partners, and employees who want to better understand, evaluate, and explore deployment requirements and best practices of PowerProtect Data Manager. Familiarity with PowerProtect DD series appliances is required.

Revisions

Date	Description
July 2019	Initial release
October 2020	Revision
July 2021	Revision
July 2022	Content update
December 2022	Updates to hyperlinks and scalability limits; template and editorial updates

We value your feedback

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

Author: Vino Jeyakanth

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

PowerProtect Data Manager overview

PowerProtect Data Manager integrates multiple data protection products within the Dell Data Protection portfolio to enable data protection as a service. PowerProtect Data Manager enables new data paths with provisioning, automation, and scheduling that enable a data protection team to embed protection engines into their infrastructure for high-performance backup and recovery.

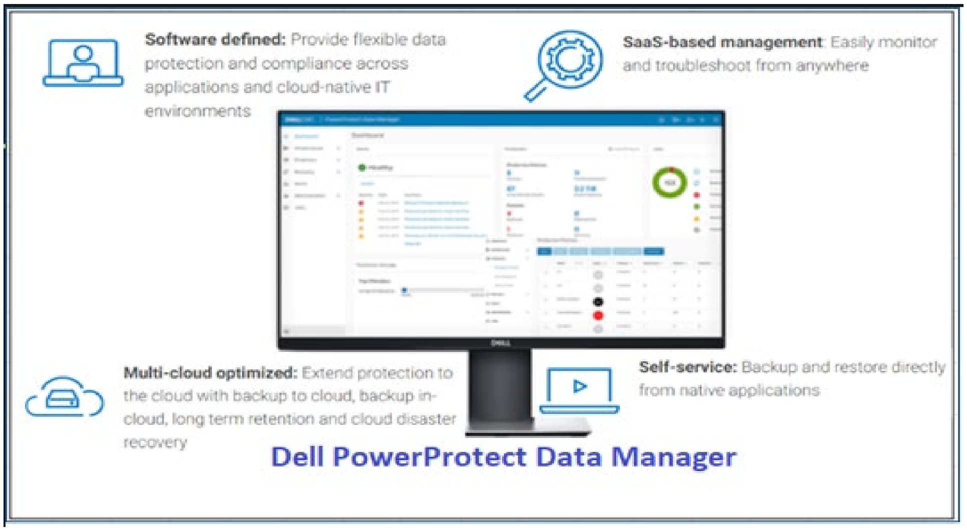

Software defined: Provide flexible data protection and compliance across applications and cloud-native IT environments
SaaS-based management: Easily monitor and troubleshoot from anywhere
Multi-cloud optimized: Extend protection to the cloud with backup to cloud, backup in-cloud, long term retention and cloud disaster recovery
Self-service: Backup and restore directly from native applications
Dell PowerProtect Data Manager

Figure 1. PowerProtect Data Manager overview

PowerProtect Data Manager offers the following benefits:

- Uses an agent-based approach to discover the protected and unprotected databases on an application server.
- Enables governed self-service and centralized protection by:
  - Monitoring and enforcing Service Level Objectives (SLOs)
  - Identifying violations of Recovery Point Objectives (RPO)
  - Applying retention locks on backups for all asset types
- Supports deploying an external VM Direct appliance to move data with the VM Direct Engine.
- Supports the vRealize Automation data protection extension, which enables provisioning of virtual machines with Data Manager protection, manual backup, and restore to the original or a new location.

- Supports integration of Cloud Disaster Recovery (Cloud DR), including workflows for Cloud DR deployment, protection, and recovery operations in the AWS or Azure cloud.
- Enables backup administrators of large-scale environments to schedule backups for the following asset types from a central location on the PowerProtect Data Manager server:
  - VMware virtual machines
  - File systems
  - VMAX storage groups
  - Kubernetes clusters
  - Microsoft Exchange and SQL databases
  - Oracle databases
  - SAP HANA databases
  - Network-attached storage (NAS) shares
- For details about version support and compatibility, see the *PowerProtect Data Manager Compatibility Matrix*.
- Supports PowerProtect Search, which enables backup administrators to quickly search for and restore VM file copies. The Search Service can be enabled by adding a search node to the configurable Search Engine that is auto deployed during the Data Manager installation.
- Provides a RESTful interface that allows the user to monitor, configure, and orchestrate Data Manager. Customers can use the APIs to integrate their own automation framework or quickly write new scripts with the help of easy to-follow tutorials.

PowerProtect Data Manager deployment methods

Introduction to deployment methods

You can deploy PowerProtect Data Manager using an Open Virtualization Appliance (OVA) or a machine image. Each method has its own considerations for the deployment itself and the functionality of PowerProtect Data Manager after its deployment.

OVA deployments

Considerations of OVA deployments include the following:

- PowerProtect Data Manager can be deployed to on-premises virtual hosts or to cloud-based environments that include VMware Cloud on Dell, VMware Cloud (VMC) on Amazon Web Services (AWS), and Azure VMware Solution (AVS) on Microsoft Azure.
- OVAs are deployed using the vSphere Client.
- Deployed PowerProtect Data Manager instances do not detect their environment. The environment must be manually selected during the deployment process for the instances to be appropriately configured.

- PowerProtect Data Manager and DDVE cannot be deployed simultaneously from the same interface.

Machine-image deployments

For machine-image deployments, consider the following information:

- PowerProtect Data Manager can only be deployed to virtual hosts on Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Product (GCP). These virtual hosts cannot be in an environment that includes VMware Cloud (VMC) or Azure VMware Solution (AVS), although any deployed PowerProtect Data Manager can still protect resources in those environments.
- Machine images are deployed using the web-based user interface of a cloud provider.
- Deployed PowerProtect Data Manager instances detect their environment and are automatically appropriately configured.
- PowerProtect Data Manager and DDVE can be deployed simultaneously and from the same interface.

This white paper describes how to deploy PowerProtect Data Manager using an OVA. For information about how to deploy PowerProtect Data Manager using a machine image, see the following guides:

- *PowerProtect Data Manager Amazon Web Services Deployment Guide*
- *PowerProtect Data Manager Azure Deployment Guide*
- *PowerProtect Data Manager Google Cloud Platform Deployment Guide*

PowerProtect Data Manager deployment considerations

Deployment introduction

Planning the environment for deploying PowerProtect Data Manager using OVA plays an important prerequisite function. You must plan for adequate resources to achieve optimal performance of PowerProtect Data Manager.

Planning VMware vCenter resources

PowerProtect Data Manager Appliance

The following table outlines the minimum resource requirements to deploy a PowerProtect Data Manager OVA in VMware vSphere 6.0 and later:

Table 1. Resource requirements for PowerProtect Data Manager OVA deployment in vSphere 6.0 and later

Specification	Value
CPU	10 CPU cores
Memory	24 GB RAM
Disk	• Disk 1: 100 GB • Disk 2: 500 GB • Disk 3 and 4: 10 GB each • Disk 5–7: 7 GB each

Specification	Value
Virtual Disk Format	Thick provision lazy zeroed
Network interface card (NIC)	1 GB
Internet Protocol	IPv4 only
For application-aware backup on VM	• vCenter version 6.5 or later • VMware ESXi server version 6.5 or later • VMware tool version 10.1 or later
For Cloud DR	• 14 CPU cores (10 for PowerProtect Data Manager and 4 for Cloud DR) • 28 GB RAM (24 GB for PowerProtect Data Manager and 4 GB for Cloud DR)

PowerProtect Search Engine

The PowerProtect Search Engine enables backup administrators to quickly search and restore VM file copies. The Search Service can be enabled by adding a search node to the configurable Search Engine that is auto deployed during PowerProtect Data Manager installation.

The PowerProtect Search Engine indexes virtual machine file metadata to enable searches based on configurable parameters. To use this feature, add at least one search engine node to the Search Engine to form a search cluster. Adding a node enables the indexing feature.

Each search engine node must meet the following system requirements:

Table 2. System requirements for search engine node

Specification	Value
CPU	4 vCPU * 2 GHz (4 virtual sockets, 1 core for each socket)
Memory	8 GB RAM
Disk	• Three disks - 50 GB each • One disk - 1 TB
Internet Protocol	IPv4 only
Network interface card (NIC)	One vmxnet3 NIC with one port

Note: You can add up to a maximum of five search engine nodes for a single PowerProtect Data Manager. One search node can index maximum 1 billion files or 1,000 virtual machines.

PowerProtect VM Direct protection engine

PowerProtect Data Manager comes prebundled with an embedded VM Direct Engine. The engine is automatically used as a fallback proxy for performing backup and restore operations when the added external proxies fail or are disabled. The VM Direct Engine facilitates data movement for both virtual machine protection policies and Kubernetes cluster protection policies.

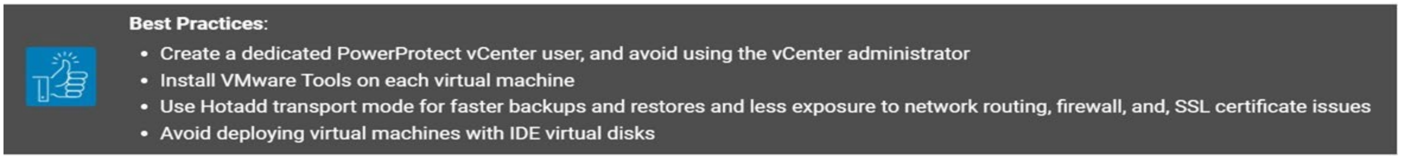
Dell Technologies recommends that you always deploy an external protection engine, also known as a VM proxy, because the embedded proxy has limited capacity for performing parallel backups. The following table details the requirements for the external VM Direct Engine:

Table 3. External VM Direct Engine requirements

Specification	Value
CPU	4 vCPU * 2 GHz (4 virtual sockets, 1 core for each socket)
Memory	8 GB RAM
Disk	Disk 1: 59 GB Disk 2: 98 GB
Internet Protocol	IPv4 only
Network interface card (NIC)	One vmxnet3 NIC with one port
SCSI controller	4 (maximum)

Notes:

- Total number of external VM Direct Engines supported with a single vCenter server is 25, although the recommended number is 7.
- Network settings such as Gateway, IP Address, Netmask, and Primary DNS are important to specify.
- Each external VM Direct Engine can manage a maximum of 25 VM backup and recovery sessions.
- The embedded VM Direct Engine supports four backup and restore sessions.



Best Practices:

- Create a dedicated PowerProtect vCenter user, and avoid using the vCenter administrator
- Install VMware Tools on each virtual machine
- Use Hotadd transport mode for faster backups and restores and less exposure to network routing, firewall, and, SSL certificate issues
- Avoid deploying virtual machines with IDE virtual disks

Planning the protection storage

PowerProtect Data Manager integrates multiple data protection products within the Dell Data Protection portfolio to enable data protection as a service. It enables new data paths with provisioning, automation, and scheduling that allow a data protection team to embed protection engines into the infrastructure for high-performance backup and recovery.

The PowerProtect Data Manager UI enables users with administrator credentials to add the following storage types:

- PowerProtect DD Management Center
- External PowerProtect DD series appliance

Note: You can also add a DD system in High Availability (HA) mode.

The following table shows the supported versions of DD series appliances:

Table 4. Supported versions of DD series appliances

PowerProtect DD series appliance	Supported versions
Hardware	DD990, DD4500, DD7200, DD9500, DD6300, DD6800, DD9300, DD9800, DD3300
Operating system	DDOS 6.1.2 or higher
PowerProtect DD Management Center (DDMC)	DDMC 6.1.0.x, 6.1.x with DDOS 6.1.x and higher
DD Virtual Edition (DDVE)	DDVE 4.0 and above

Best Practice: Create a dedicated PowerProtect Data Domain BOOST user and avoid using sysadmin account for Data Domain discovery.

Note: When a PowerProtect DD Management Center is added, PowerProtect Data Manager discovers all the supported DD series appliances that are managed by the PowerProtect DD Management Center.

Planning networking

The following sections outline the networking requirements for deploying PowerProtect Data Manager.

IP and DNS requirement

Networking requirements are as follows:

- Unique IP addresses must be allocated to the PowerProtect Data Manager, VM Search Engine, and VM Direct Engine. Only IPV4 IP addresses are supported.
- NTP servers are recommended to sync PowerProtect Data Manager with NTP server.
- DNS server and default gateway servers should also be specified during install. You can configure up to three DNSs.
- Forward and reverse DNS lookups are recommended.
- When configuring PowerProtect Data Manager, do not use an IP address in the 172.24.0.192 /26 subnet. IP addresses from 172.24.0.192 through 172.24.0.255 are reserved for the private Docker network.
- vCenter registration and proxy deployment fail if the PowerProtect Data Manager server is deployed in the same private network as the internal Docker network.

Firewall and port requirements

PowerProtect Data Manager is a single node in a virtual appliance that uses the Linux SLES 12 firewall to protect and limit external access to the system. PowerProtect Data Manager uses a direct socket connection to communicate and move data internally and across the network to the required service with minimal overhead.

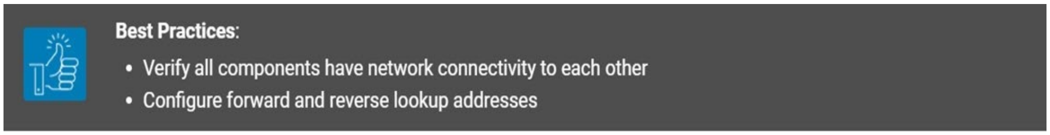
To enable communication between the PowerProtect Data Manager system and other applications, PowerProtect Data Manager configures firewall rules for ports that are used for inbound and outbound communication. The following table shows the port requirements for PowerProtect Data Manager:

Table 5. PowerProtect Data Manager port requirements

Description	Communication	Port
SSH communications	Bi-directional communication between the SSH client and the PowerProtect Data Manager appliance	22 TCP/UDP
SQL, Oracle, Exchange, SAP HANA, file system	Bi-directional communication between the PowerProtect Data Manager agent and the PowerProtect Data Manager appliance Requirement applies to Application Direct and VM Direct.	7000 TCP
REST server	Bi-directional communication between the HTTP client and the PowerProtect Data Manager appliance	8443 TCP
RESTAPI server – VM Direct	Bi-directional communication between the PowerProtect Data Manager agent and the PowerProtect Data Manager appliance Requirement applies to SQL VM application aware.	8443 TCP
UI redirect	Inbound only	• 80 TCP • 443
LDAP	Outbound only	• 389 TCP/UDP • 636 TCP
Discovery (devices)	Outbound between the PowerProtect Data Manager appliance and the device	• 3009 TCP—Storage Direct and DD system • 5989 TCP—SMI-S • 443 TCP—XtremIO • 7225 TCP—RecoverPoint
PowerProtect Data Manager agent	Bi-directional communication between the database hosts and the PowerProtect Data Manager appliance This requirement applies to both Application Direct and VM Direct.	7000 TCP
Embedded VM Direct service	Outbound	9090 TCP

Description	Communication	Port
PowerProtect controller	Outbound between the PowerProtect Data Manager appliance and PowerProtect Controller on the Kubernetes cluster PowerProtect Data Manager uses this port to pull the logs from the controller pod.	30095 TCP
PowerProtect DD series appliance	Bi-directional port should be open between DD series appliance and External VM Direct or application hosts.	• 111 TCP • 2049 TCP • 2052 TCP
vCenter	Bi-directional between the PowerProtect Data Manager and vCenter for discovery, initiating Hot Add transport mode, restores including Instant access restore.	• 443 HTTPS • 7444 TCP

Note: To get a detailed list, see the *PowerProtect Data Manager Security Configuration Guide*.



Best Practices:

- Verify all components have network connectivity to each other
- Configure forward and reverse lookup addresses

Planning application hosts

Dell Technologies recommends preinstalling the supported application agents:

- PowerProtect Data Manager Oracle RMAN Agent
- PowerProtect Data Manager Microsoft Exchange server Agent
- PowerProtect Data Manager Microsoft SQL server Agent
- PowerProtect Data Manager File System Agent
- PowerProtect Data Manager SAP HANA Agent

User permission requirements for supported platforms

The following table shows an overview of the permissions requirements for all supported platforms.

Note: Check individual guides for more details about permissions for each workload.

Table 6. User permissions requirements for supported platforms

Application workload	User permissions requirements				Documentation
	Installation and discovery	Backup: Self-service	Backup: Centralized	Recovery	
SQL – Application Direct	Any user with local administrator privileges	Any user with local administrator privileges	Any user with local administrator privileges	Any user with local administrator privileges	PowerProtect Data Manager Microsoft Application Agent SQL Server User Guide

SQL – Application Aware	Any user with local administrator privileges	Not applicable	Any user with local administrator privileges	Any user with local administrator privileges	PowerProtect Data Manager Microsoft Application Agent SQL Server User Guide
Microsoft Exchange	Any user with local administrator privileges Note: To create a user using the App Agent Exchange Admin Configuration tool, log in with domain administrator permissions.	Exchange User configured using the App Agent Exchange Admin Configuration tool	Exchange User configured using the App Agent Exchange Admin Configuration tool	Exchange User configured using the App Agent Exchange Admin Configuration tool OR Any specific user group privileges to the system account and user account that will perform the restore operations	PowerProtect Data Manager Microsoft Application Agent Exchange Server User Guide
SAP HANA	Operating system root user	• System database: System database user with backup administrator, catalog read role • Tenant database: Either system database user with database administrator role or tenant database administrator with backup administrator, catalog read roles	• HANA studio: System database: System database user with backup administrator, catalog read role Tenant database: Either system database user with database administrator role or tenant database administrator with backup administrator, catalog read roles • HANA CLI Hana (<sid>adm) user from CLI	Database administrator or Hana <sid>adm operating system user	PowerProtect Data Manager SAP HANA Agent User Guide

Oracle	Oracle user for RMAN agent install (.install.sh) And Operating system root user for agent service (PowerProtect Agent RPM)	Oracle operating system user (by default) OR Oracle database user (Oracle 12c and later sysbackup privilege is required of any database user) Precedence (high to low): Wallet/DB/OS Authentication	Oracle operating system user (by default) OR Oracle database user (Oracle 12c and later sysbackup privilege is required of any database user) Precedence (high to low): Wallet/DB/OS Authentication	Oracle operating system user (by default) OR Oracle database user (Oracle 12c and later sysbackup privilege is required of any database user) Precedence (high to low): Wallet/DB/OS Authentication	PowerProtect Data Manager Oracle RMAN Agent User Guide
File system	• For Linux: Operating system root user • For Windows: Any user with local administrator privileges	• For Linux: Root user • For Windows: Any user with local administrator privileges	• For Linux: Root user • For Windows: Any user with local administrator privileges	• For Linux: Root user • For Windows: Any user with local administrator privileges	PowerProtect Data Manager File System User Guide
VMware	A vCenter user account at the root level of the vCenter that is strictly dedicated for use with VM Direct protection engine Note: Avoid using vCenter administrator account.	Not applicable	Dedicated vCenter user account at the root level of vCenter Note: The User Guide provides a full list of user account privileges.	• Full VM restore: Dedicated vCenter user account at the root level of vCenter • FLR restore: Any user with local administrator privileges	PowerProtect Data Manager Virtual Machine User Guide
Storage Direct	For Linux – root user For Windows- Any user with local administrator privileges	Ddboost and DdVdiskUser specified in the lockbox configuration file must have the administrator role.	Ddboost and DdVdiskUser specified in the lockbox configuration file must have the administrator role.	Ddboost and DdVdiskUser specified in the lockbox configuration file must have the administrator role.	PowerProtect Data Manager Storage Direct User Guide

To provide local administrator privileges correctly to a domain user on Windows server:

1. On the Active Directory server, create a domain user account (dns\domain user) or use an existing domain user.
2. Make the user a member of "Backup Operations" and "Remote Desktop Users."
3. Log in to the application host as system administrator.
4. Go to **Control Panel** > **User Accounts** > **Manage User Accounts**, and add the new user with local administrator privileges.
5. Click **Start** > **Administrative Tools** > **Local Security Policy** > **User Rights Assignment** > **Log on as a Service**, and add the new user.
6. Disable UAC.

This domain user account can now be used to perform SQL, Exchange, and file system application agent installations.

Planning licensing

The available license types are as follows.

- **Trial**: Applied automatically on installation of PowerProtect Data Manager and enabling full use of the product for up to 90 days without applying a license key. When the trial period ends, PowerProtect Data Manager continues to operate with full functionality so that you can apply a permanent license.
- **Front-end protected capacity by terabyte (FETB)**: The primary model of e-Licensing, which is based on the capacity that you want to protect. For example, you can purchase a 100 TB license, which enables you to protect up to 100 TB of data.
- **Socket-based**: Licensed per CPU socket on virtual machine hosts that are being backed up or replicated.

Note: When upgrading from a previous release, any existing license, and its associated Secure Remote Services connections (SupportAssist replaces Secure Remote Services in PowerProtect Data Manager 19.8.) care removed from the system and replaced with a 90-day trial license. Therefore, a valid FETB license for PowerProtect Data Manager and any associated Secure Remote Services connections must be reinstalled.

To obtain the XML license file from the Dell license management website, you must have the License Authorization Code (LAC), which is emailed from Dell. If the LAC is misplaced or not received, contact a Dell technical support representative.

Deployment of PowerProtect Data Manager

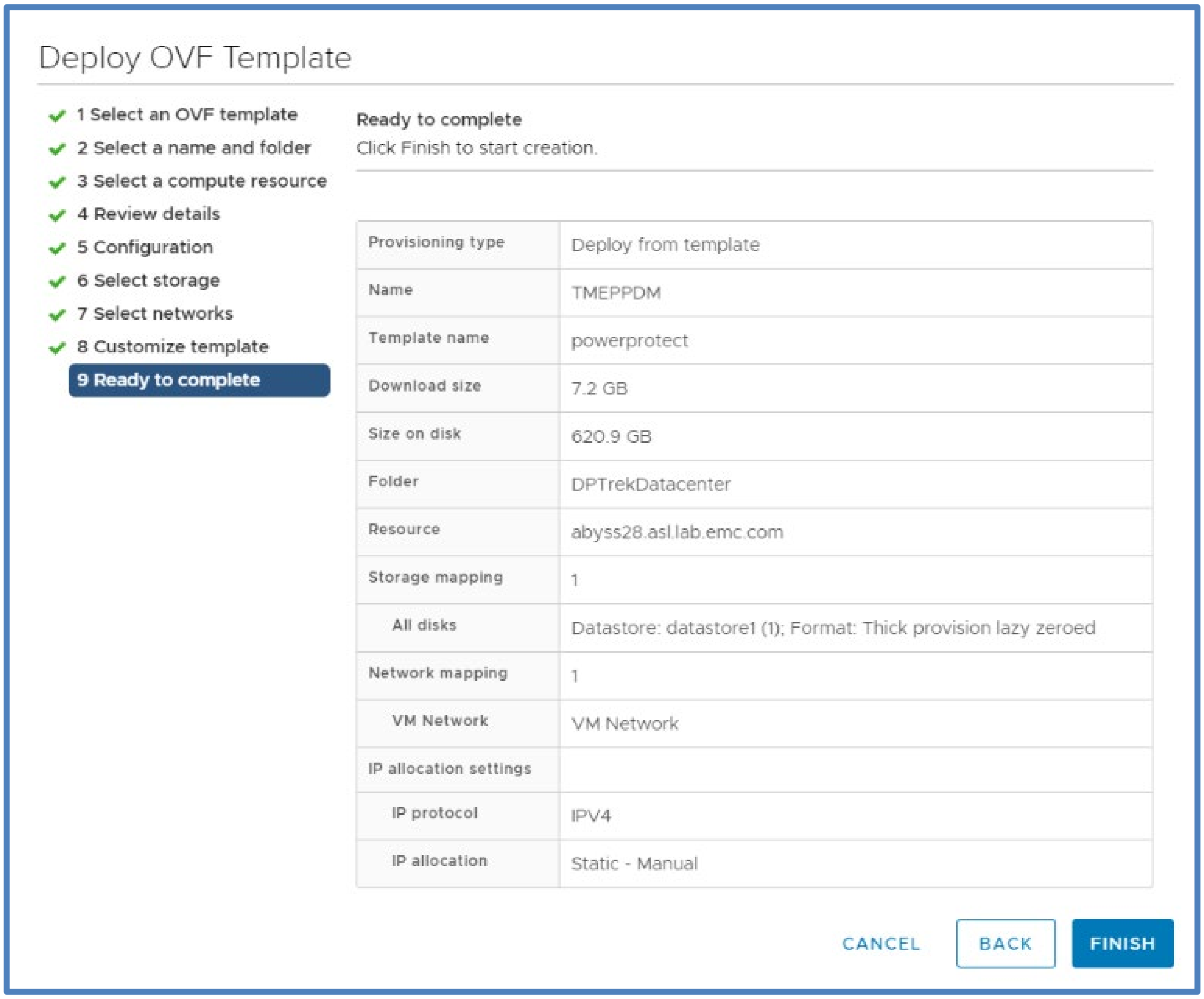
PowerProtect Data Manager Appliance is easy to install and configure. The PowerProtect Data Manager Open Virtual Appliance (OVA) can be deployed using one of the following methods:

- Manually deploying the OVA to a vCenter server—Use this method to deploy the OVA to a stand-alone or cluster host, while logged into the vCenter server. Configuration of the network settings is supported during the deployment.

- Manually deploying the OVA to an ESXi host—Use this method to deploy the OVA while logged in to an ESXi host. Use the VM console to configure the network settings after the deployment completes.

Note: Enter the network details correctly in the network section of the OVA deployment flow; otherwise, the appliance will not connect after deployment.

Once the PowerProtect Data Manager OVA deployment is completed, all the services and components of the software are accessible.



Ready to complete

Click Finish to start creation.

Provisioning type	Deploy from template
Name	TMEPPDM
Template name	powerprotect
Download size	7.2 GB
Size on disk	620.9 GB
Folder	DPTrekDatacenter
Resource	abyss28.asl.lab.emc.com
Storage mapping	1
All disks	Datastore: datastore1 (1); Format: Thick provision lazy zeroed
Network mapping	1
VM Network	VM Network
IP allocation settings	
IP protocol	IPV4
IP allocation	Static - Manual

Figure 2. PowerProtect Data Manager OVF deployment

Post-installation steps for PowerProtect Data Manager

Once the PowerProtect Data Manager OVA is successfully deployed and the VM is powered on, you can access the PowerProtect Data Manager UI. Enter the IP address or FQDN configured during the deployment using https://*appliance_hostname.*

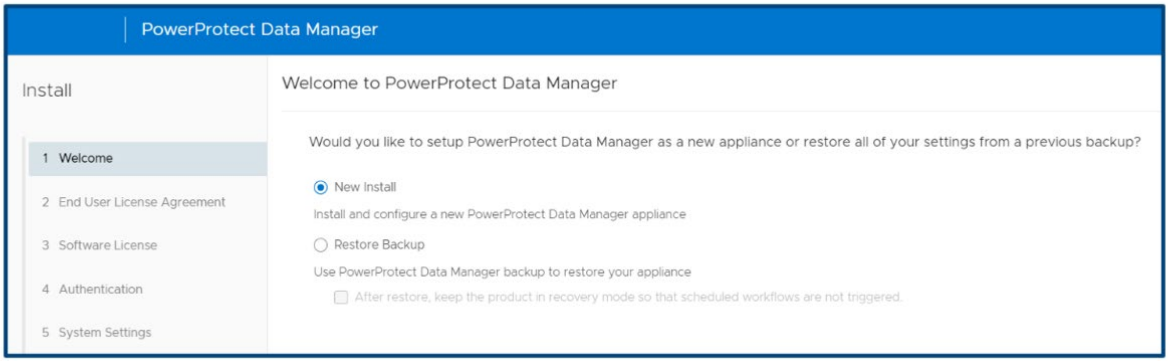
The security certificate that encrypts communication between the PowerProtect Data Manager UI and the web browser is self-signed. A self-signed certificate has been signed by the web server that hosts the secure web page being viewed by a web browser. This certificate is enough to establish an encrypted channel between the web browser and the server. However, it has not been signed by a trusted authority.

The next step is to configure the basic settings for the PowerProtect Data Manager. Google Chrome is the only supported browser.

Welcome screen

The **Welcome** screen is displayed when the PowerProtect UI is accessed for the first time after deploying the OVF template. There are two options available on this screen: New Install and Restore Backup.

- **New Install**: If you are installing the device for the first time, click **New Install**.
- **Restore Backup**: This option is used when PowerProtect Data Manager appliance must be restored from a previous backup. To delay jobs defined by your protection policies until otherwise specified, select the option **After restoring, keep the product in recovery mode so that scheduled workflows are not triggered**. A system alert is displayed in the PowerProtect Data Manager.



Welcome to PowerProtect Data Manager

Would you like to setup PowerProtect Data Manager as a new appliance or restore all of your settings from a previous backup?

● New Install

Install and configure a new PowerProtect Data Manager appliance

○ Restore Backup

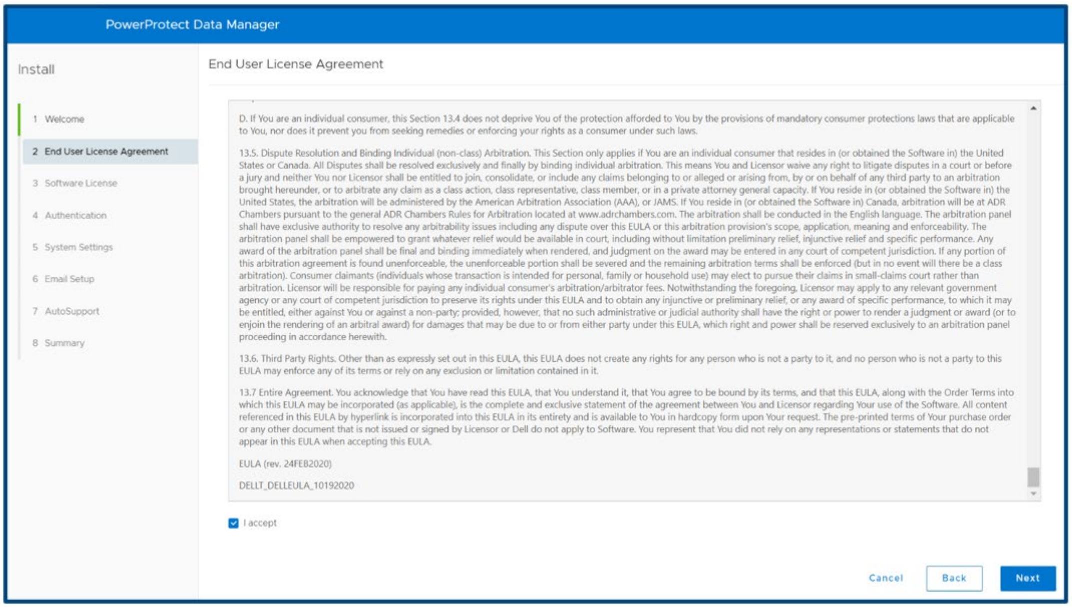
Use PowerProtect Data Manager backup to restore your appliance

□ After restore, keep the product in recovery mode so that scheduled workflows are not triggered.

Figure 3. PowerProtect Data Manager welcome screen

End-user license agreement (EULA)

Scroll through the agreement and accept the license.



End User License Agreement

D. If You are an individual consumer, this Section 13.4 does not deprive You of the protection afforded to You by the provisions of mandatory consumer protections laws that are applicable to You, nor does it prevent you from seeking remedies or enforcing your rights as a consumer under such laws.

13.5. Dispute Resolution and Binding Individual (non-class) Arbitration. This Section only applies if You are an individual consumer that resides in (or obtained the Software in) the United States or Canada. All Disputes shall be resolved exclusively and finally by binding individual arbitration. This means You and Licensor waive any right to litigate disputes in a court or before a jury and neither You nor Licensor shall be entitled to join, consolidate, or include any claims belonging to or alleged or arising from, by or on behalf of any third party to an arbitration brought hereunder, or to arbitrate any claim as a class action, class representative, class member, or in a private attorney general capacity. If You reside in (or obtained the Software in) the United States, the arbitration will be administered by the American Arbitration Association (AAA), or JAMS. If You reside in (or obtained the Software in) Canada, arbitration will be at ADR Chambers pursuant to the general ADR Chambers Rules for Arbitration located at www.adrchambers.com. The arbitration shall be conducted in the English language. The arbitration panel shall have exclusive authority to resolve any arbitrability issues including any dispute over this EULA or this arbitration provision's scope, application, meaning and enforceability. The arbitration panel shall be empowered to grant whatever relief would be available in court, including without limitation preliminary relief, injunctive relief and specific performance. Any award of the arbitration panel shall be final and binding immediately when rendered, and judgment on the award may be entered in any court of competent jurisdiction. If any portion of this arbitration agreement is found unenforceable, the unenforceable portion shall be severed and the remaining arbitration terms shall be enforced (but in no event will there be a class arbitration). Consumer claimants (individuals whose transaction is intended for personal, family or household use) may elect to pursue their claims in small-claims court rather than arbitration. Licensor will be responsible for paying any individual consumer's arbitration/arbitrator fees. Notwithstanding the foregoing, Licensor may apply to any relevant government agency or any court of competent jurisdiction to preserve its rights under this EULA and to obtain any injunctive or preliminary relief, or any award of specific performance, to which it may be entitled, either against You or against a non-party; provided, however, that no such administrative or judicial authority shall have the right or power to render a judgment or award (or to enjoin the rendering of an arbitral award) for damages that may be due to or from either party under this EULA, which right and power shall be reserved exclusively to an arbitration panel proceeding in accordance herewith.

13.6. Third Party Rights. Other than as expressly set out in this EULA, this EULA does not create any rights for any person who is not a party to it, and no person who is not a party to this EULA may enforce any of its terms or rely on any exclusion or limitation contained in it.

13.7 Entire Agreement. You acknowledge that You have read this EULA, that You understand it, that You agree to be bound by its terms, and that this EULA, along with the Order Terms into which this EULA may be incorporated (as applicable), is the complete and exclusive statement of the agreement between You and Licensor regarding Your use of the Software. All content referenced in this EULA by hyperlink is incorporated into this EULA in its entirety and is available to You in hardcopy form upon Your request. The pre-printed terms of Your purchase order or any other document that is not issued or signed by Licensor or Dell do not apply to Software. You represent that You did not rely on any representations or statements that do not appear in this EULA when accepting this EULA.

EULA (rev. 24FEB2020)

DELLT_DELLEULA_10192020

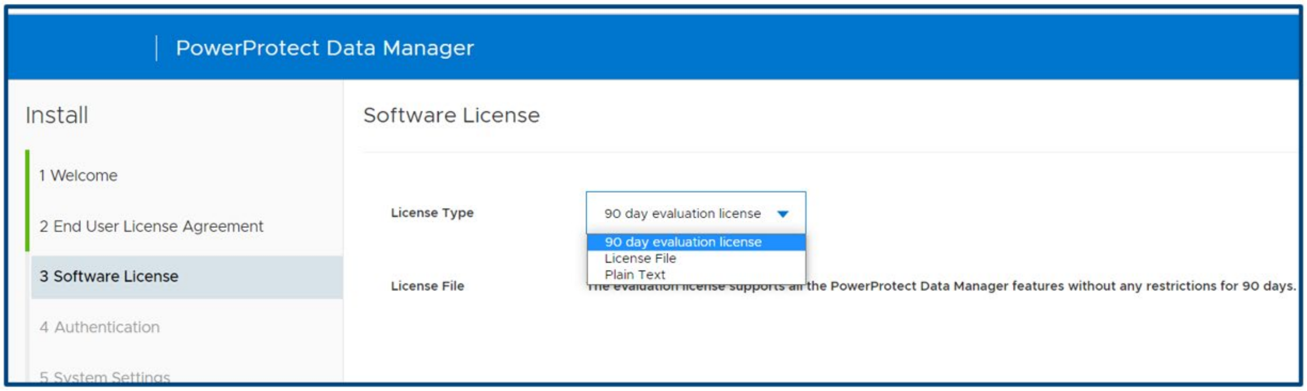
☑ I accept

Figure 4. PowerProtect Data Manager EULA

License

PowerProtect Data Manager has three types of license-trial license (valid for 90 days), Front-End Terabyte (FTEB) protected capacity and socket-based.

The relevant .xml license file can be obtained from the Dell license management website. To obtain the license file, you must have the License Authorization Code (LAC), which was emailed from Dell. If you have not received the LAC, contact your technical support representative.



Software License

License Type: 90 day evaluation license

License File: The evaluation license supports all the PowerProtect Data Manager features without any restrictions for 90 days.

Figure 5. PowerProtect Data Manager license type selection

Authentication

The authentication screen allows the administrator to set an authentication password for appliance management. In addition, the administrator can set the same password or a different one using the toggle key option for the root, administrator, and support accounts for Linux, SSH, and support activities.

From the PowerProtect Data Manager CLI, password expiry can be set to never for users such as administrator, root, and support accounts by running the following command:

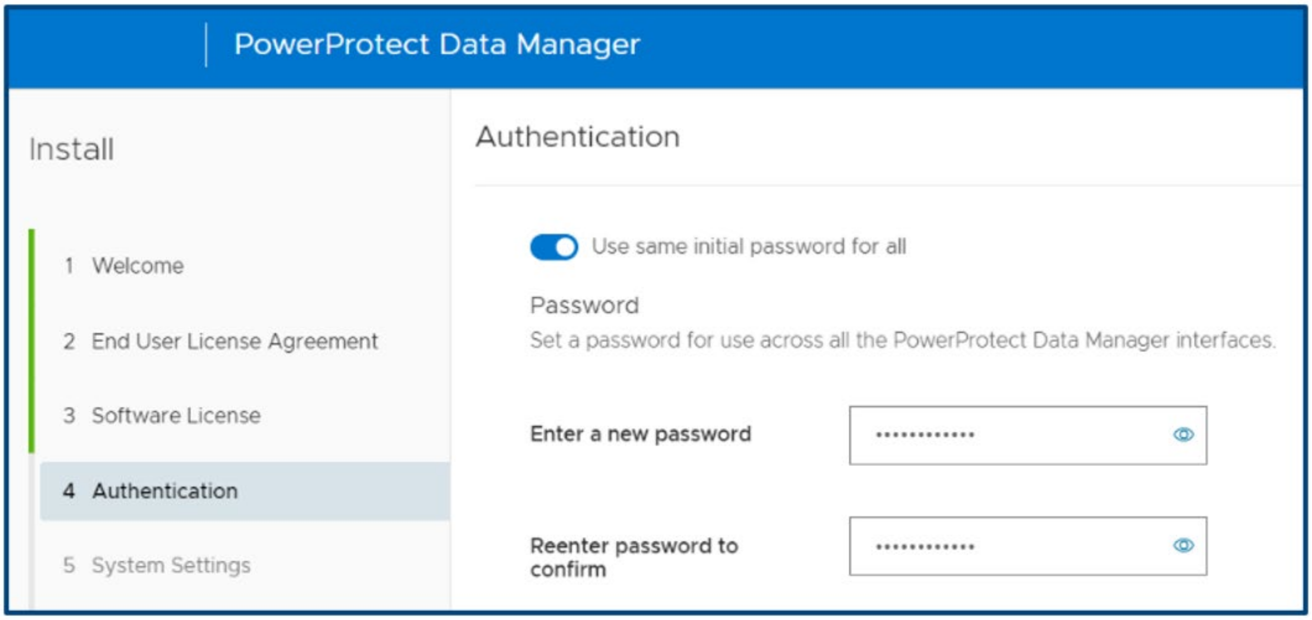
```
chage -m 0 -M 99999 -I -1 -E -1 <role-name>
```

- The administrator password is used to log in to the PowerProtect Data Manager management console.

Note: PowerProtect Data Manager application user's password is set to 60 days by default. To extend the expiration time, update the value of the parameter `aaa.server.policies.password.maxAge` in the properties file: `/usr/local/brs/lib/aaa/config/application-policies-custom.properties`

- The service password is used to log in to SSH for support activities.
- The lockbox password is used during restore operations.

Note: You can select **Use of the same password for all** to set the same password for administrator, service, and lockbox accounts, but it is not recommended. Save all the passwords securely for later use.



Authentication

● Use same initial password for all

Password

Set a password for use across all the PowerProtect Data Manager interfaces.

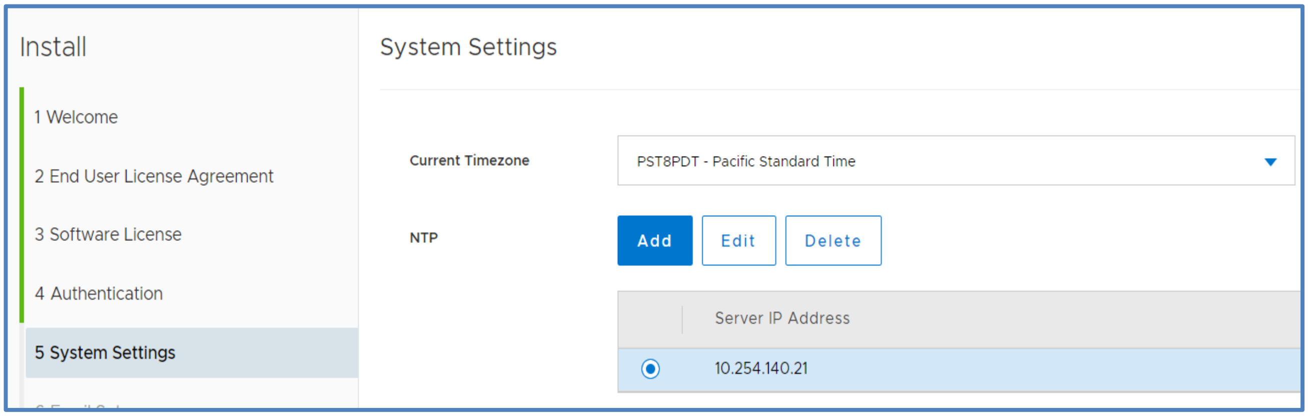
Enter a new password: •••••••••••••

Reenter password to confirm: •••••••••••••

Figure 6. PowerProtect Data Manager authentication

System settings

The system settings screen allows the user to add the NTP server. Dell Technologies recommends that users always add an NTP server and sync the PowerProtect Data Manager with it.



System Settings

Current Timezone: PST8PDT - Pacific Standard Time

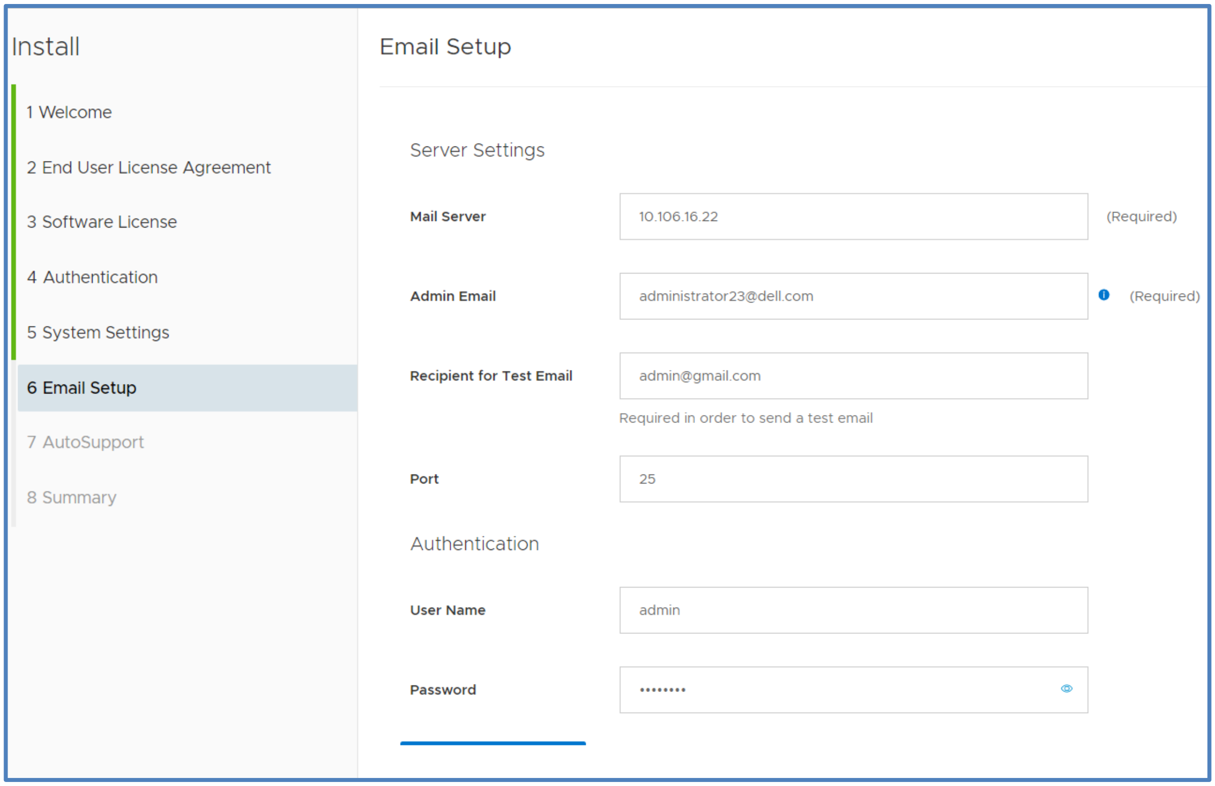
NTP

	Server IP Address
●	10.254.140.21

Figure 7. PowerProtect Data Manager system settings

Email and SMTP setup

Email setup is an optional step. The SMTP server can be configured to receive the PowerProtect Data Manager alerts using a specified email address. To send diagnostic and usage data to Dell for proactive support and to help improve our products and services, switch Auto Support to ON.



Email Setup

Server Settings

Mail Server: 10.106.16.22 (Required)

Admin Email: administrator23@dell.com (Required)

Recipient for Test Email: admin@gmail.com

Required in order to send a test email

Port: 25

Authentication

User Name: admin

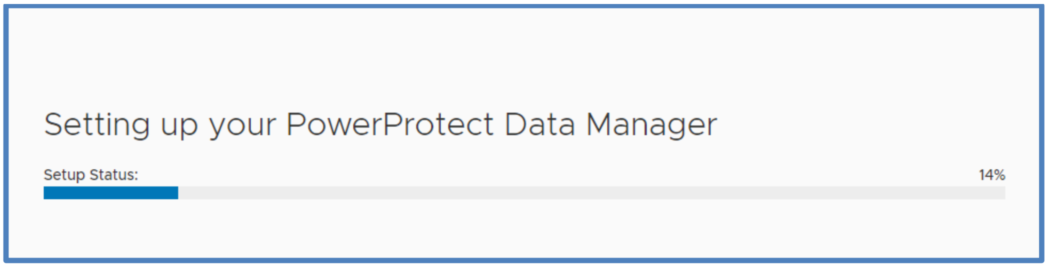
Password: ••••••••

Figure 8. PowerProtect Data Manager email setup (optional)

Login and Getting Started

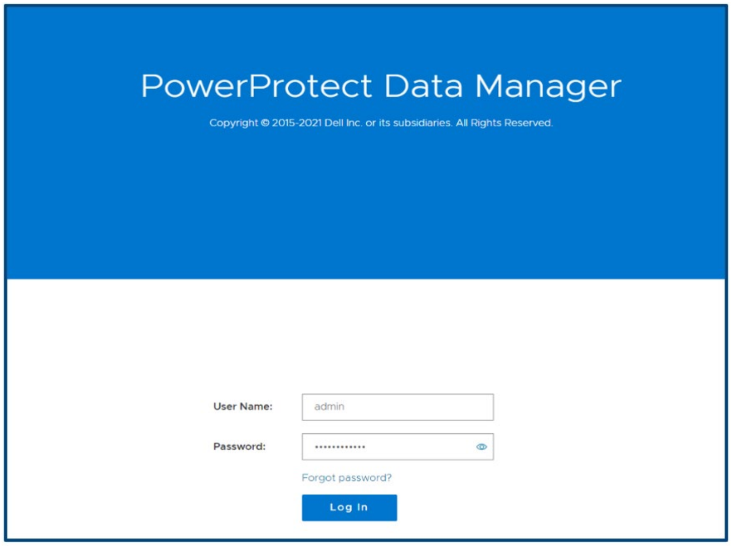
Once the DONE button on the summary screen is selected, the PowerProtect Data Manager applies all the configured settings, and the login screen is displayed after the setup is complete.

A user can now log in to the PowerProtect Data Manager using the credentials specified in the authentication step. The default login username is `admin`.


Setting up your PowerProtect Data Manager

Setup Status: 14%

Figure 9. PowerProtect Data Manager configuration in progress



PowerProtect Data Manager

Copyright © 2015-2021 Dell Inc. or its subsidiaries. All Rights Reserved.

User Name: admin

Password: ••••••••••••

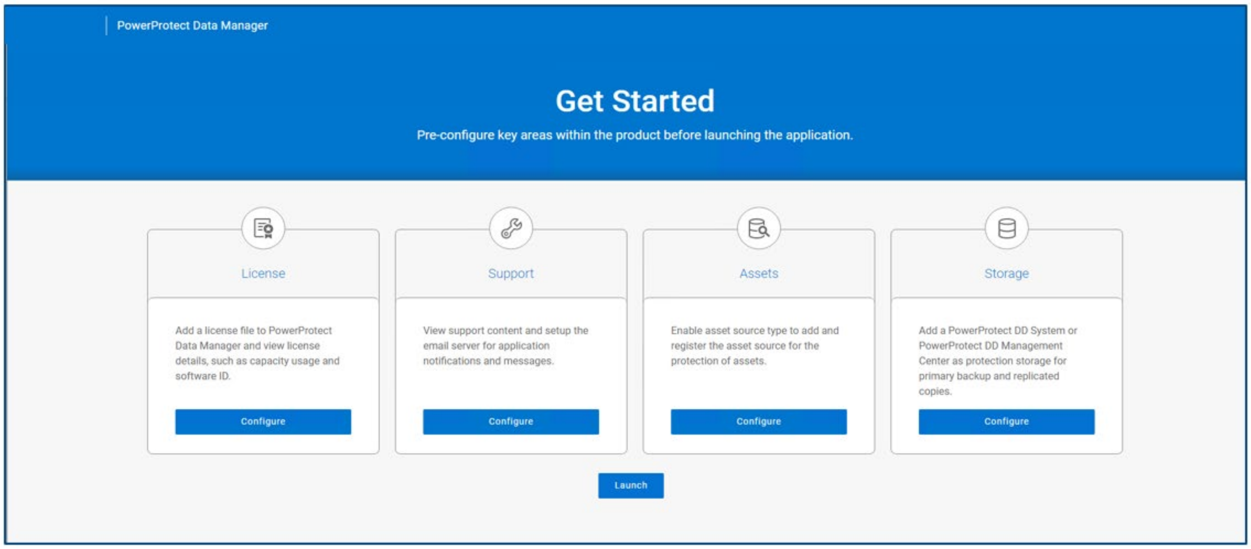
Figure 10. PowerProtect Data Manager login screen

After logging in, the **Get Started** screen is visible. The PowerProtect Data Manager returns to the **Get Started** screen until you click **Skip This**.

The **Get Started** screen can be accessed at any time through **System Settings** > **Getting Started**. The navigation options on the **Get Started** screen are:

- **License**: Links to the License addition page
- **Support**: Links to the SupportAssist configuration page
- **Assets**: Links to the Asset sources page.
- **Storage**: Links to the target Storage Addition or configuration page

Click **Launch** to skip this step and go to the main UI.



PowerProtect Data Manager

Get Started

Pre-configure key areas within the product before launching the application.

License

Add a license file to PowerProtect Data Manager and view license details, such as capacity usage and software ID.

Support

View support content and setup the email server for application notifications and messages.

Assets

Enable asset source type to add and register the asset source for the protection of assets.

Storage

Add a PowerProtect DD System or PowerProtect DD Management Center as protection storage for primary backup and replicated copies.

Figure 11. PowerProtect Data Manager Get Started screen

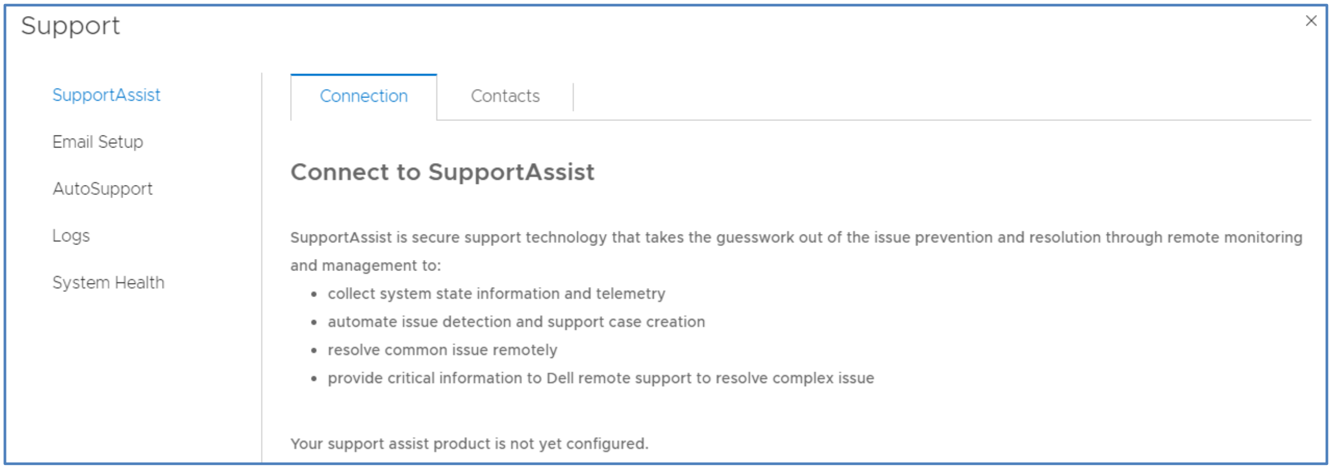
Configure SupportAssist for PowerProtect Data Manager

SupportAssist is a support tool that communicates with PowerProtect Data Manager to monitor your environment, automatically detect current and potential issues, and collect and store diagnostic data. SupportAssist securely sends the data that is required for troubleshooting an issue to Technical Support for diagnostic purposes and Customer Support.

SupportAssist provides the following features and benefits:

- Proactive monitoring and issue prevention
- Facilitates upgrade package downloads
- Automatic support case creation based on event alerting
- Automatic health checks
- Communicates telemetry data
- Real-time troubleshooting
- Customer support

Note: SupportAssist provides automated support capabilities for PowerProtect Data Manager systems. SupportAssist replaces Secure Remote Services in the current release of PowerProtect Data Manager. If you have configured Secure Remote Services previously, the PowerProtect Data Manager system automatically migrates Secure Remote Services to SupportAssist when you upgrade the PowerProtect Data Manager. SupportAssist cannot be configured when you have a trial license.



Connect to SupportAssist

SupportAssist is secure support technology that takes the guesswork out of the issue prevention and resolution through remote monitoring and management to:

- collect system state information and telemetry
- automate issue detection and support case creation
- resolve common issue remotely
- provide critical information to Dell remote support to resolve complex issue

Your support assist product is not yet configured.

Figure 12. Connecting to SupportAssist

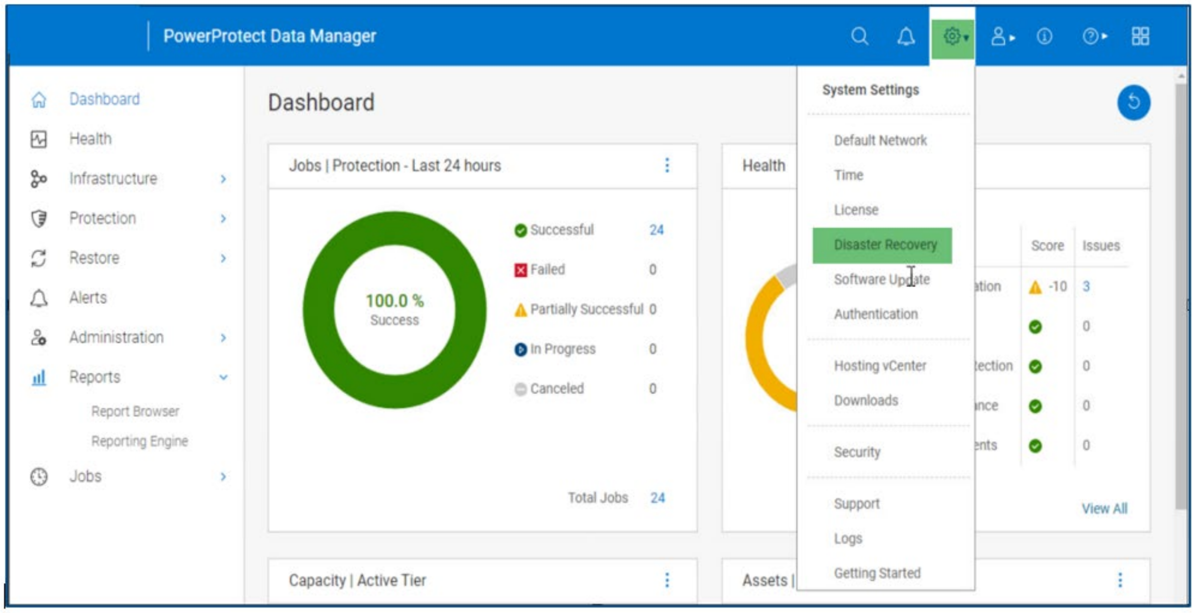
An access key and PIN are required to configure a secure connection between PowerProtect Data Manager and SupportAssist. You must apply the access key and PIN once.

For details, see *PowerProtect Data Manager Deployment Guide* to complete this setup.

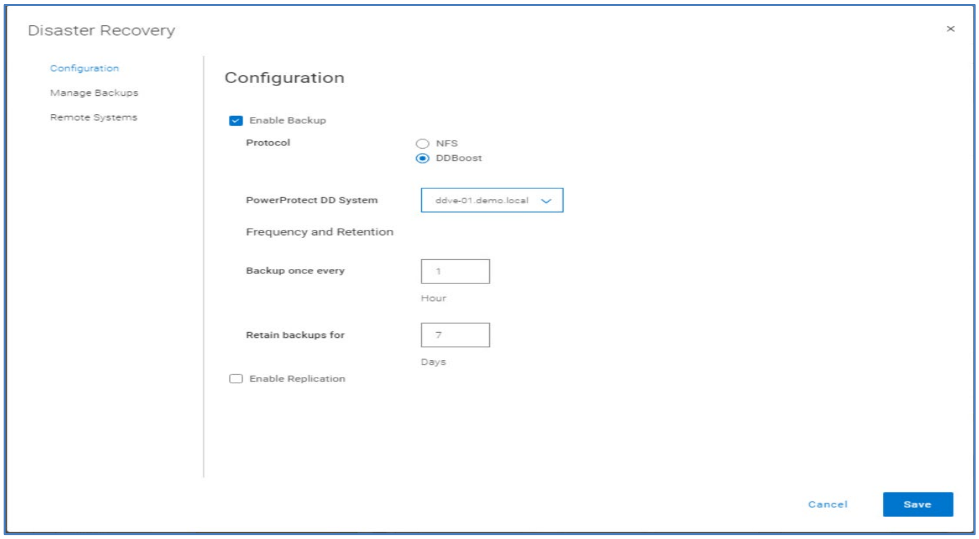
Setting up disaster recovery of PowerProtect Data Manager

The PowerProtect Data Manager system protection service enables you to protect the persistent data of a PowerProtect Data Manager system from catastrophic loss by creating a series of system backups.

- Each backup is considered a “full” backup although it is created in an incremental manner. The persistent data that is saved in a backup includes the Lockbox and Elasticsearch databases.
- The backup operation creates a Point-in-Time snapshot of the database while the system is in a quiesced state. While the system is quiesced, user functionality is limited. After the snapshot is completed, and while PowerProtect Data Manager copies the snapshots to the DD storage unit, full user functionality is restored. If the system fails to quiesce, PowerProtect Data Manager still takes a backup, which is marked as crash consistent instead of application consistent.
- To store system backups, you must configure and assign a private DD storage unit for the PowerProtect Data Manager system. The system protection service enables you to manage the frequency and start time of an automated system backup, perform manual backups, and define the length of time that the system backups are available for recovery.



- File Search indexes are backed up for DR recovery along with other component DR backups.
- Make the following selections, and then click **Save**.
  - Select **Enable Backup**.
  - At **Protocol**, select **NFS** or **DDBoost**. (DDBoost is recommended.)
  - At **PowerProtect DD System**, select the system from the drop-down menu if it has already been added; otherwise, add a PowerProtect DD appliance.



Configuration

☑ Enable Backup

Protocol ○ NFS ● DDBoost

PowerProtect DD System: ddve-01.demo.local

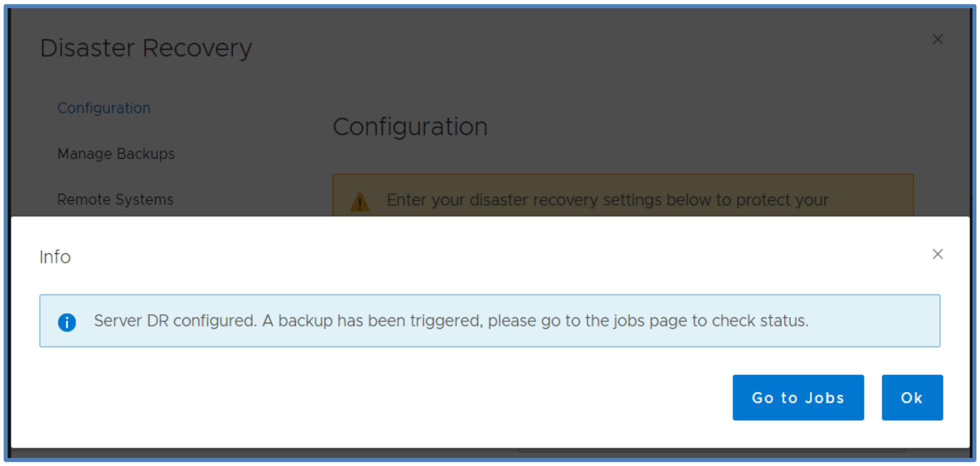
Frequency and Retention

Backup once every: 1 Hour

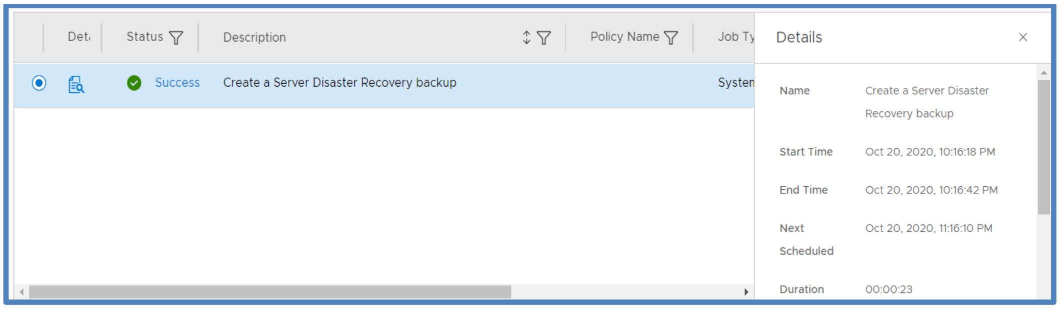
Retain backups for: 7 Days

□ Enable Replication

The initial backup runs, and then backups are automatically triggered every hour.



Server DR configured. A backup has been triggered, please go to the jobs page to check status.



	Deta	Status	Description	Policy Name	Job Ty
●		Success	Create a Server Disaster Recovery backup		Systen

Name	Create a Server Disaster Recovery backup
Start Time	Oct 20, 2020, 10:16:18 PM
End Time	Oct 20, 2020, 10:16:42 PM
Next Scheduled	Oct 20, 2020, 11:16:10 PM
Duration	00:00:23

Add asset sources

In PowerProtect Data Manager, assets are the basic units that PowerProtect Data Manager protects. Asset sources are the mechanism that PowerProtect Data Manager uses to manage assets and communicate with the storage system where backup copies of the assets are stored.

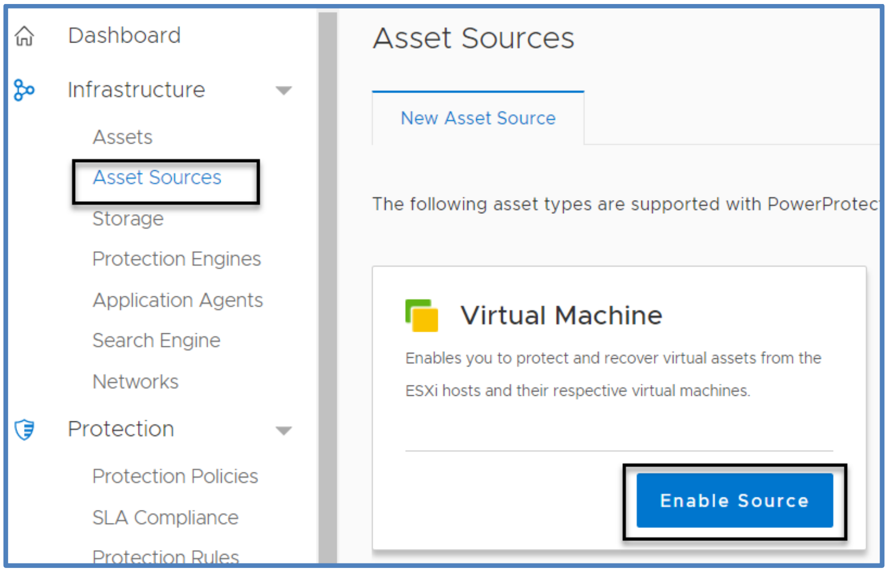
Asset sources can be a vCenter Server, Kubernetes cluster, application host, or SMIS server. Assets can be Virtual Machines, Exchange databases, SQL databases, Oracle databases, SAP HANA databases, File systems, Kubernetes namespaces, or Storage Groups.

Add a vCenter Server

An asset source, such as a vCenter Server, must be enabled in PowerProtect Data Manager before you can add and register the asset source for the protection of assets.

Follow these steps to add a vCenter Server as an asset source in the PowerProtect Data Manager UI:

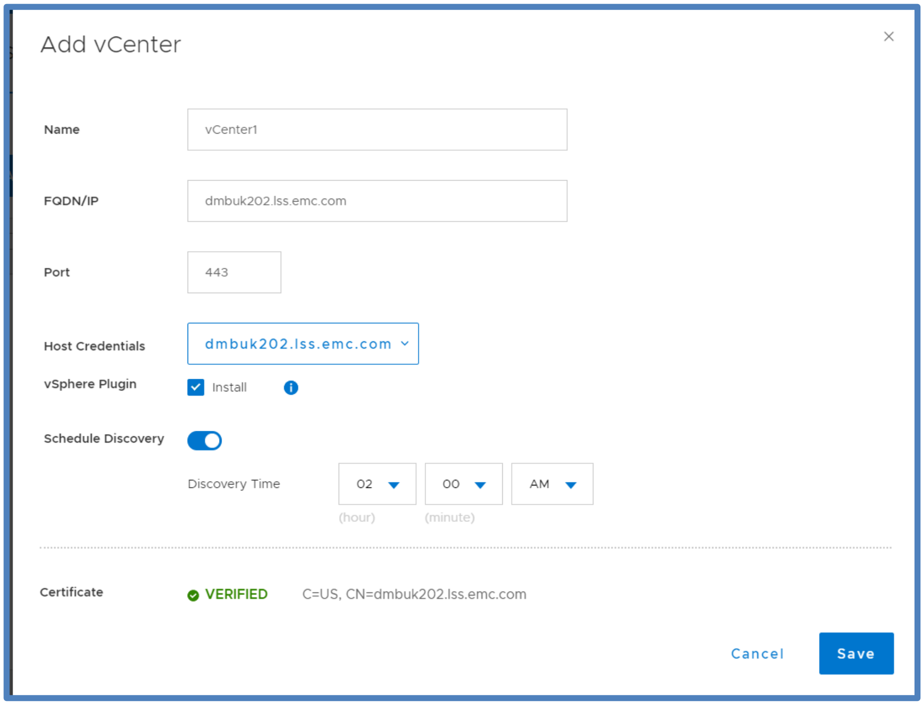
1. Select **Infrastructure** > **Asset Sources** > **Virtual Machine** > **Enable Source**.



The following asset types are supported with PowerProtec

Enables you to protect and recover virtual assets from the ESXi hosts and their respective virtual machines.

2. Enter the vCenter details and click **Save**.



Name: vCenter1

FQDN/IP: dmbuk202.lss.emc.com

Port: 443

Host Credentials: dmbuk202.lss.emc.com

vSphere Plugin: ☑ Install

Schedule Discovery: ●

Discovery Time: 02 (hour) 00 (minute) AM

Certificate: VERIFIED C=US, CN=dmbuk202.lss.emc.com

The initial vCenter Server discovery identifies all VMware ESXi clusters, hosts, and virtual machines within the vCenter Server. Subsequent discoveries are performed automatically according to a fixed interval to identify any additional or changed VMware entities since the last discovery operation. You can also manually initiate a discovery of VMware entities at any time from the **vCenter** tab of the **Asset Sources** window by selecting a vCenter Server and clicking **Discover**.

After the vCenter virtual machine assets are discovered, you can add a VM Direct appliance to facilitate data movement and then create virtual machine protection policies to back up these assets.

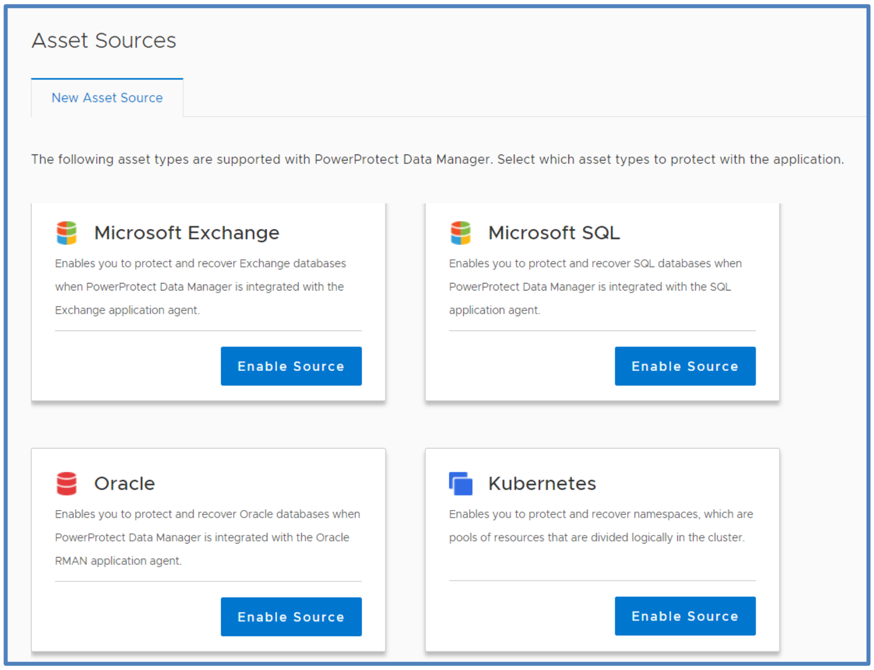
Add other asset sources

In addition to vCenter Server asset sources, PowerProtect Data Manager provides the option to enable the following asset sources to protect application assets.

- Kubernetes Cluster
- File System Agent
- Microsoft Exchange Agent
- Microsoft SQL Agent
- Oracle RMAN Agent
- SAP HANA Agent
- Storage Direct Agent for Storage Data Management

Note: This white paper does not provide instructions for each application agent. For links to the individual application agent user guides, see User permission requirements for supported platforms.

Select **Infrastructure** > **Asset Sources** > **Enable Source**.



Asset Sources

New Asset Source

The following asset types are supported with PowerProtect Data Manager. Select which asset types to protect with the application.

Microsoft Exchange

Enables you to protect and recover Exchange databases when PowerProtect Data Manager is integrated with the Exchange application agent.

Enable Source

Microsoft SQL

Enables you to protect and recover SQL databases when PowerProtect Data Manager is integrated with the SQL application agent.

Enable Source

Oracle

Enables you to protect and recover Oracle databases when PowerProtect Data Manager is integrated with the Oracle RMAN application agent.

Enable Source

Kubernetes

Enables you to protect and recover namespaces, which are pools of resources that are divided logically in the cluster.

Enable Source

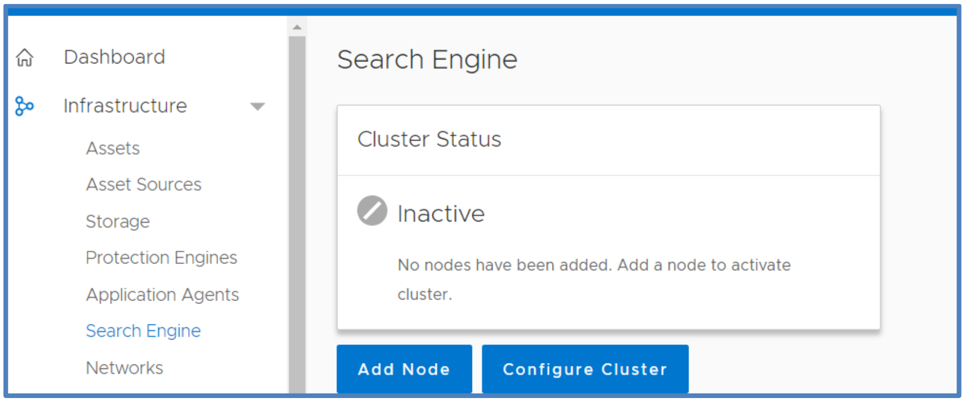
Configuring PowerProtect Search Engine

When you install PowerProtect Data Manager version 19.3 or later, the PowerProtect Search Engine is installed by default. The following bullet points explain its usage:

- The PowerProtect Search Engine indexes virtual machine file metadata to enable searches based on configurable parameters. To use this feature, add at least one search engine node to the Search Engine to form a search cluster, and then enable the indexing feature.
- PowerProtect Search is an optional feature that can be enabled, set up, and configured for virtual machine backups and protection policies. When you enable this feature, a backup of the Search Engine is taken as part of the server backup process.
- As of this release, you cannot disable these backups. When Search is enabled, you must allow the Search Engine virtual machine on the DD series appliance that contains the Server Backup MTree: Add the search node IP address or hostname to the client list for the NFS export.

Add and configure the Search Engine as follows:

1. To add the Search Engine, select **Infrastructure** > **Search Engine** and click **Add Node**.



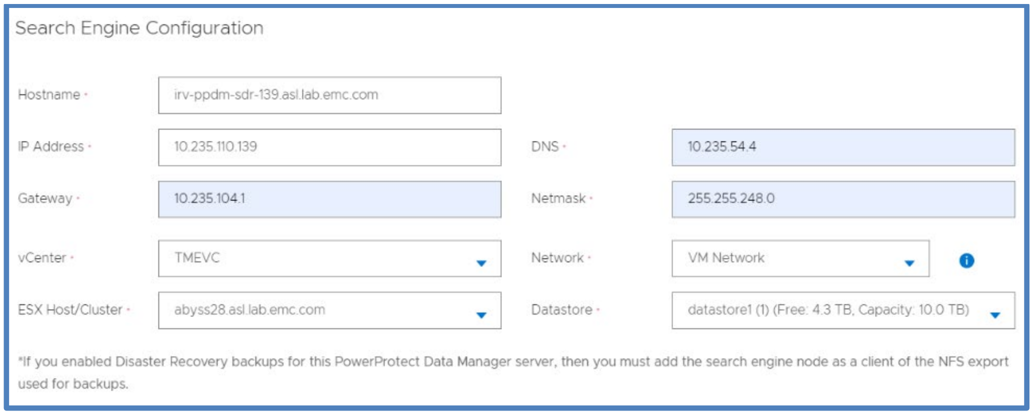
Search Engine

Cluster Status

Inactive

No nodes have been added. Add a node to activate cluster.

2. In the **Add Search Engine Node** dialog box, enter the required network parameters.

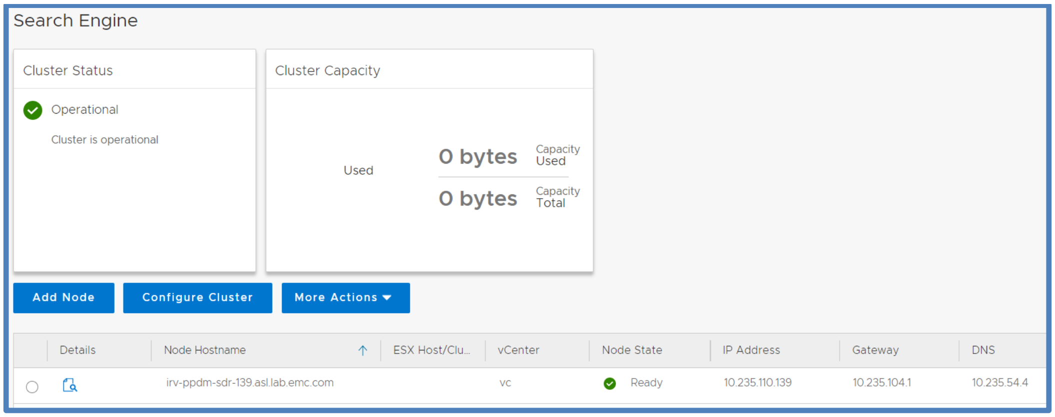


Search Engine Configuration

Hostname *	irv-ppdm-sdr-139.asl.lab.emc.com		
IP Address *	10.235.110.139	DNS *	10.235.54.4
Gateway *	10.235.104.1	Netmask *	255.255.248.0
vCenter *	TMEVC	Network *	VM Network
ESX Host/Cluster *	abyss28.asl.lab.emc.com	Datastore *	datastore1 (1) (Free: 4.3 TB, Capacity: 10.0 TB)

*If you enabled Disaster Recovery backups for this PowerProtect Data Manager server, then you must add the search engine node as a client of the NFS export used for backups.

3. Select **Add** and wait a few minutes for the VM to show the **Node State** as **Ready**.



Operational

Cluster is operational

Used

0 bytes Capacity Used

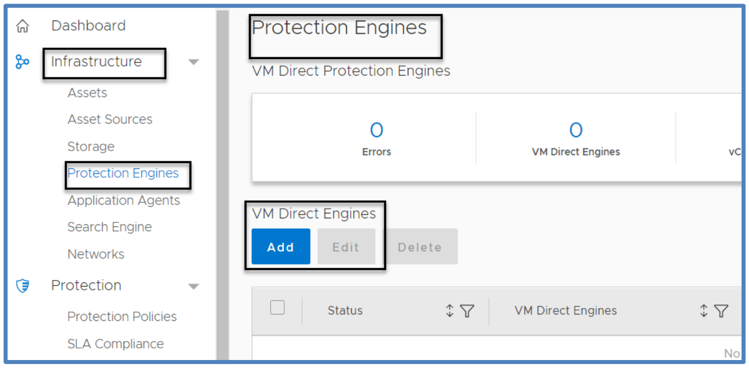
0 bytes Capacity Total

	Details	Node Hostname	ESX Host/Clu...	vCenter	Node State	IP Address	Gateway	DNS
○		irv-ppdm-sdr-139.asl.lab.emc.com		vc	✓ Ready	10.235.110.139	10.235.104.1	10.235.54.4

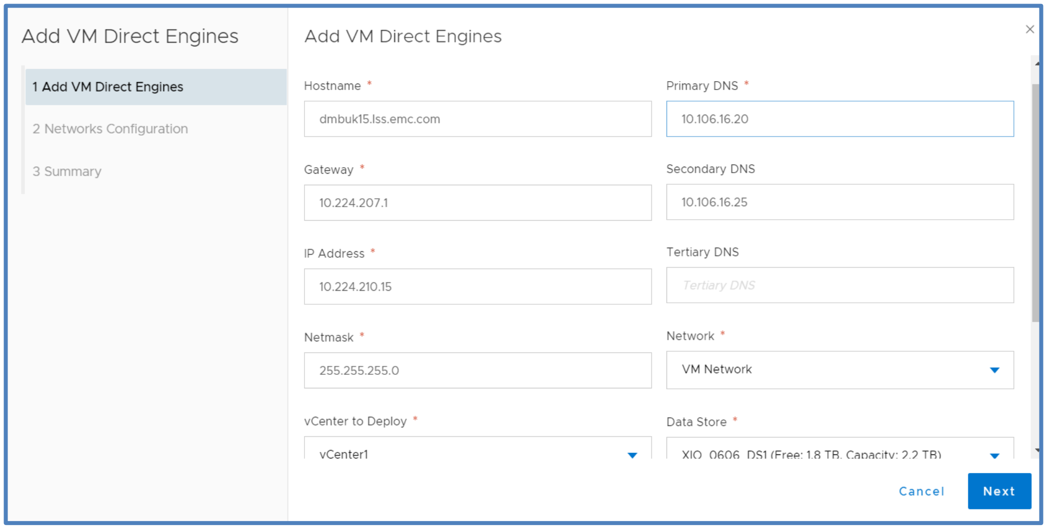
Adding external VM Direct Engine

In the **Protection Engines** window, deploy an external VM Direct Engine, also referred to as a VM proxy, to facilitate data movement for virtual machine protection policies:

1. Select **Infrastructure** > **Protection Engine** > **Add**.



2. Enter the network details and click **Next**.



Hostname * dmbuk15.lss.emc.com

Gateway * 10.224.207.1

IP Address * 10.224.210.15

Netmask * 255.255.255.0

vCenter to Deploy * vCenter1

Primary DNS * 10.106.16.20

Secondary DNS 10.106.16.25

Tertiary DNS Tertiary DNS

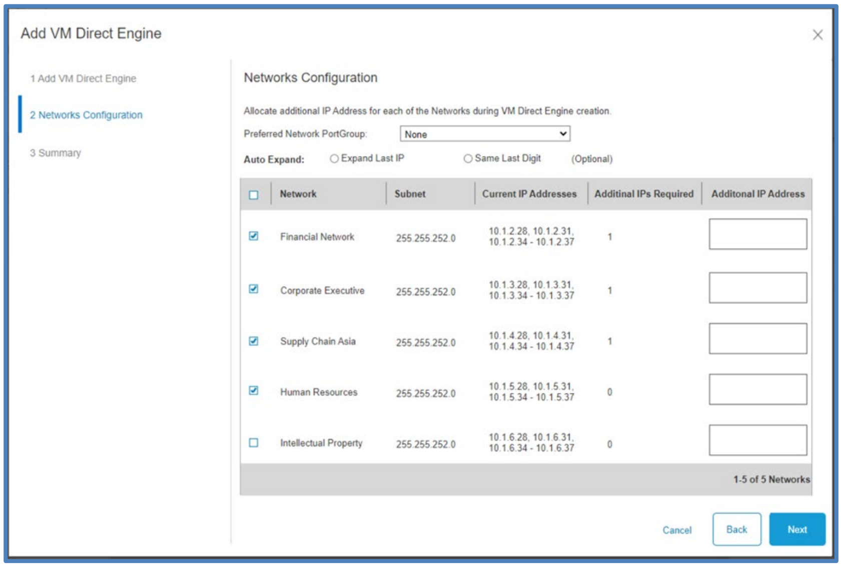
Network * VM Network

Data Store * XIO_0606_DS1 (Free: 1.8 TB, Capacity: 2.2 TB)

3. Select the VLAN network configured for the VM Direct Engine.

   For more details about adding multiple VLANs, see

Multiple VLAN configurations.



Add VM Direct Engine

1 Add VM Direct Engine
2 Networks Configuration
3 Summary

Networks Configuration

Allocate additional IP Address for each of the Networks during VM Direct Engine creation.

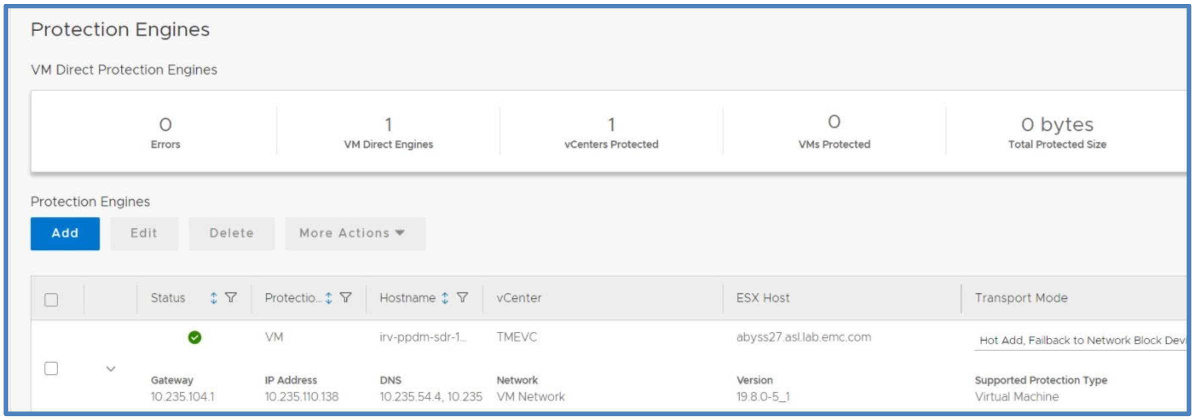
Preferred Network PortGroup: None

Auto Expand: ○ Expand Last IP ○ Same Last Digit (Optional)

□	Network	Subnet	Current IP Addresses	Additinal IPs Required	Additonal IP Address
☑	Financial Network	255.255.252.0	10.1.2.28, 10.1.2.31, 10.1.2.34 - 10.1.2.37	1	
☑	Corporate Executive	255.255.252.0	10.1.3.28, 10.1.3.31, 10.1.3.34 - 10.1.3.37	1	
☑	Supply Chain Asia	255.255.252.0	10.1.4.28, 10.1.4.31, 10.1.4.34 - 10.1.4.37	1	
☑	Human Resources	255.255.252.0	10.1.5.28, 10.1.5.31, 10.1.5.34 - 10.1.5.37	0	
□	Intellectual Property	255.255.252.0	10.1.6.28, 10.1.6.31, 10.1.6.34 - 10.1.6.37	0	

1-5 of 5 Networks

The proxy is automatically deployed on the vCenter. Once its status shows that it is ready, you can configure VM backups.



Protection Engines

VM Direct Protection Engines

0	1	1	0	0 bytes
Errors	VM Direct Engines	vCenters Protected	VMs Protected	Total Protected Size

Protection Engines

□		Status	Protectio...	Hostname	vCenter	ESX Host	Transport Mode
□	⌄	✓	VM	irv-ppdm-sdr-1...	TMEVC	abyss27.asl.lab.emc.com	Hot Add, Failback to Network Block Dev
		Gateway 10.235.104.1	**IP Address** 10.235.110.138	**DNS** 10.235.54.4, 10.235	**Network** VM Network	**Version** 19.8.0-5_1	**Supported Protection Type** Virtual Machine

Adding PowerProtect DD series appliance

The PowerProtect Data Manager UI enables users with administrator credentials to add the following storage types:

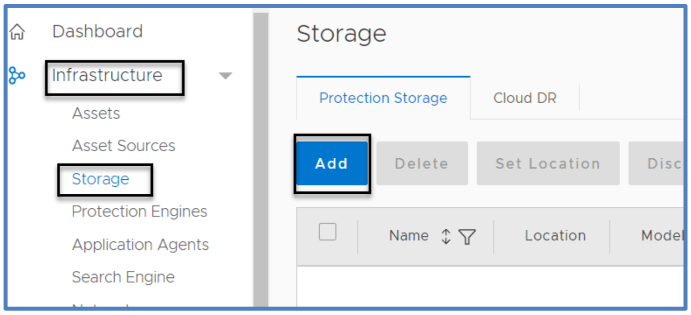
- PowerProtect DD Management Center
- External PowerProtect DD series appliance

For each PowerProtect DD series appliance, the PowerProtect DD Management Center that manages the DD system is indicated in the **Managed By** column in the table.

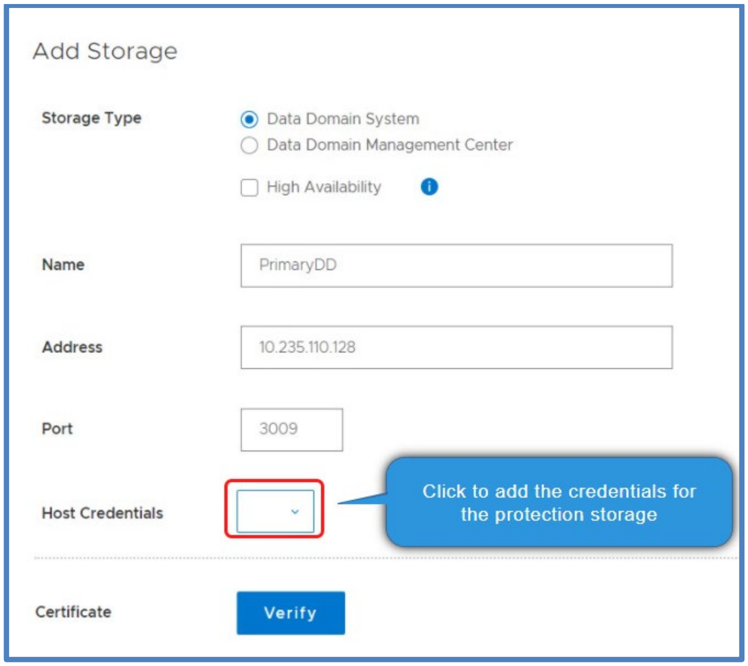
If a DD series appliance is added directly to the PowerProtect Data Manager, the name that was provided for the DD series when it was added to the PowerProtect Data Manager system is displayed in the **Managed By** column.

Add the PowerProtect DD series appliance:

1. Select **Infrastructure** > **Storage** and click **Add**.



2. Enter the DD series appliance details and click **Save**.

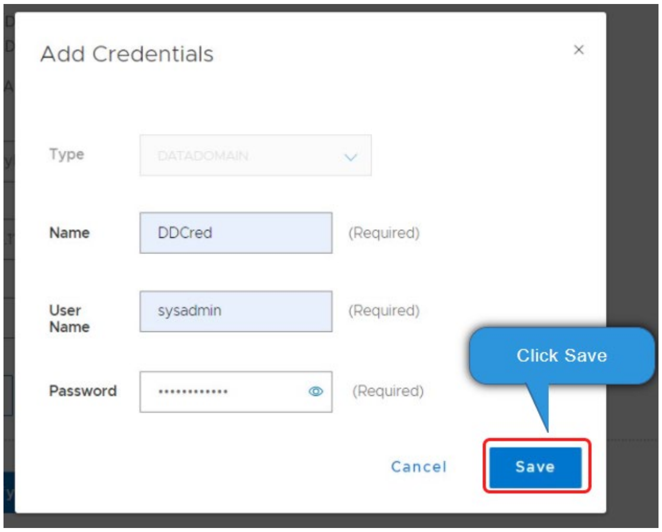


Add Storage

Storage Type	● Data Domain System ○ Data Domain Management Center □ High Availability
Name	PrimaryDD
Address	10.235.110.128
Port	3009
Host Credentials	
Certificate	Verify

Click to add the credentials for the protection storage

3. Add the host credentials and click **Save**.



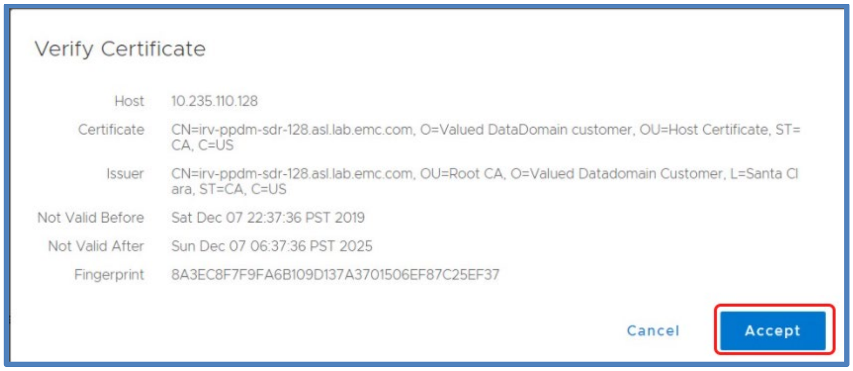
Add Credentials

Type	DATADOMAIN	
Name	DDCred	(Required)
User Name	sysadmin	(Required)
Password	•••••••••••••	(Required)

Cancel Save

Click Save

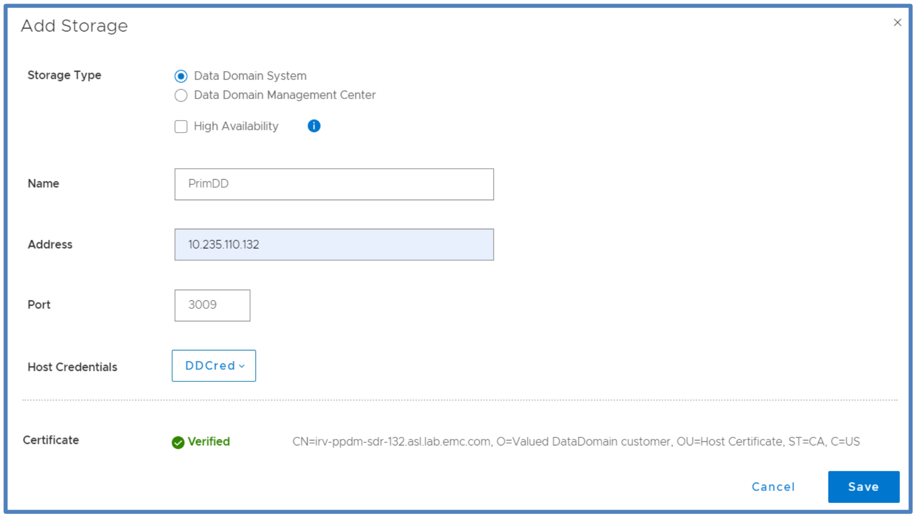
4. At **Verify Certificate**, click **Accept**.



Verify Certificate

Host	10.235.110.128
Certificate	CN=irv-ppdm-sdr-128.asl.lab.emc.com, O=Valued DataDomain customer, OU=Host Certificate, ST=CA, C=US
Issuer	CN=irv-ppdm-sdr-128.asl.lab.emc.com, OU=Root CA, O=Valued Datadomain Customer, L=Santa Clara, ST=CA, C=US
Not Valid Before	Sat Dec 07 22:37:36 PST 2019
Not Valid After	Sun Dec 07 06:37:36 PST 2025
Fingerprint	8A3EC8F7F9FA6B109D137A3701506EF87C25EF37

5. Under **Add Storage**, confirm that the certificate status is displayed as **Verified**, and then click **Save**.



Add Storage

Storage Type: ● Data Domain System ○ Data Domain Management Center

□ High Availability

Name: PrimDD

Address: 10.235.110.132

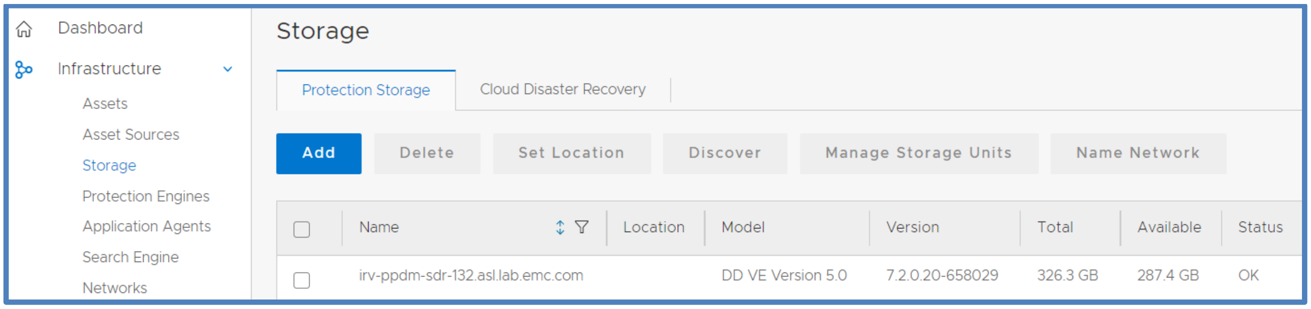
Port: 3009

Host Credentials: DDCred

Certificate: ✓ Verified CN=irv-ppdm-sdr-132.asl.lab.emc.com, O=Valued DataDomain customer, OU=Host Certificate, ST=CA, C=US

Verification

Discovery is completed within a few minutes. Verify that DD series appliance has been added to the PowerProtect Data Manager successfully by selecting **Infrastructure** > **Storage** > **Protection Storage** tab.



□	Name	Location	Model	Version	Total	Available	Status
□	irv-ppdm-sdr-132.asl.lab.emc.com		DD VE Version 5.0	7.2.0.20-658029	326.3 GB	287.4 GB	OK

You are now ready to start configuring the backups. For more information about configuring VM, file system, and application backups, along with other management activities, see the *PowerProtect Data Manager Administration and User Guide*.

Multiple VLAN configurations

Multiple VLAN configurations: Introduction and prerequisites

PowerProtect Data Manager can separate management and backup traffic onto different virtual networks (VLANs). Virtual networks help to improve data traffic routing, security, and organization.

- The default configuration routes the management traffic over the same network as backup traffic. All assets are part of the same network.
- Virtual networks can also be configured to separate management traffic from backup traffic. This configuration can also separate traffic that originates from different networks.

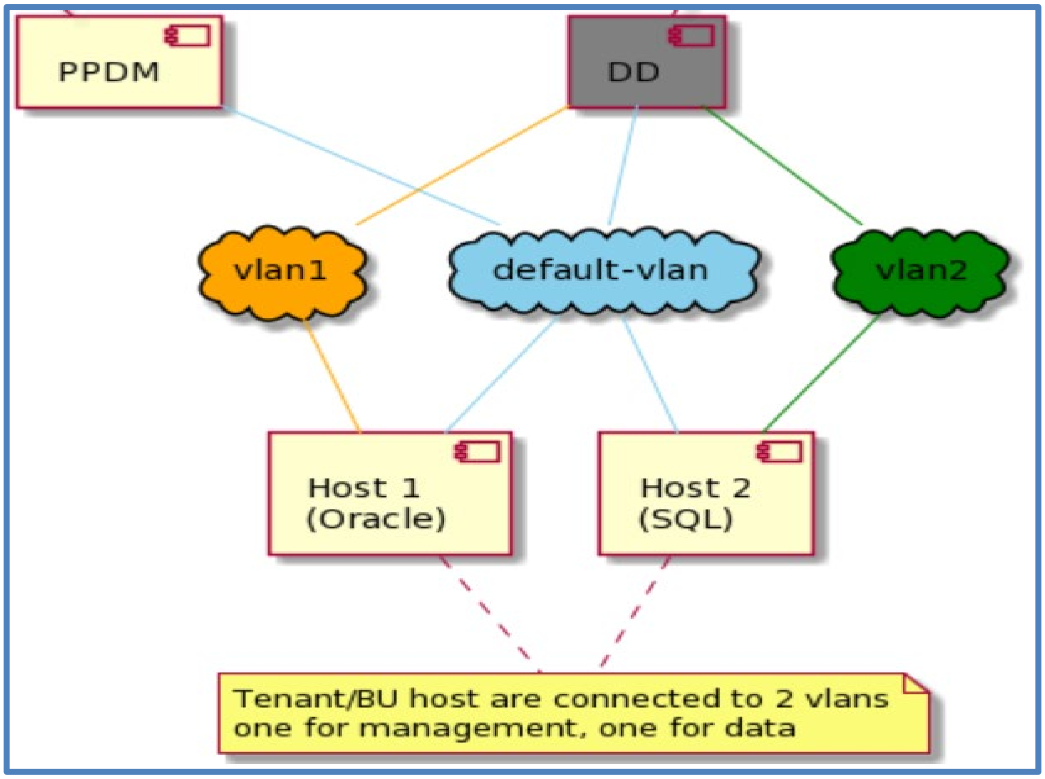

PPDM
DD
vlan1
default-vlan
vlan2
Host 1 (Oracle)
Host 2 (SQL)
Tenant/BU host are connected to 2 vlans one for management, one for data

Figure 13. Example of 2-VLAN environment

Before you configure a virtual network, complete the following actions:

1. Register the vCenter server on which the PowerProtect Data Manager is deployed. You can verify the registration on the **vCenter** tab of the **Asset Sources** page.
2. Configure the network switch port for trunk mode. This setting allows the port to carry traffic for multiple VLANs.
3. Enable Virtual Guest Tagging (VGT) mode on the VMware ESXi virtual network switch port for the PowerProtect Data Manager. Configure the virtual switch port for VLAN ID 4095.
4. Configure a VLAN interface for the DD through the **Interfaces** tab on the **Hardware** > **Ethernet** window in the DD System Manager. The DD documentation provides more information relating to this activity.

5. Add the DD series appliance as protection storage for the PowerProtect Data Manager.

Note: PowerProtect Data Manager does not verify the network switch configurations. If the physical or virtual network switch is incorrectly configured, the virtual network configuration fails.

Configuring VLAN

PowerProtect Data Manager names each virtual network in two places, the interface to the DD series appliance and the interface to the protected assets. These names are not required to match. However, Dell Technologies strongly recommends that you use the same network name in both locations for each virtual network. Record each network name for later use.

- Adding a virtual network includes creating a pool of static IP addresses. PowerProtect Data Manager uses these addresses for the local interfaces to the virtual network and for any VM Direct Engines that you deploy on this network. Ensure that you have enough IP addresses available on each network to meet this requirement. To prepare for future expansion, you can add more IP addresses than are initially required.
- The initial steps to configure and add each virtual network are one-time events. The subsequent steps to assign virtual networks to protection policies or assets happen as required.
- Configuration is nondisruptive. You can add, edit, or delete virtual networks without affecting background activities, disconnecting network interfaces, or affecting the PowerProtect Data Manager user interface.

Configuration follows a multistep workflow as follows:

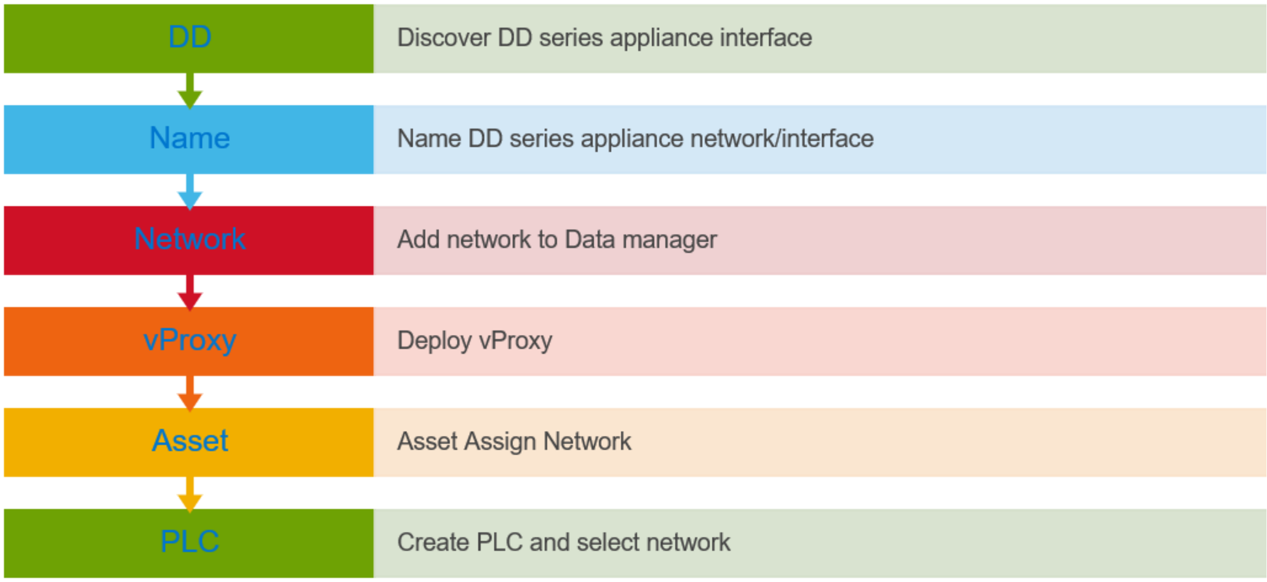

DD
Discover DD series appliance interface
Name
Name DD series appliance network/interface
Network
Add network to Data manager
vProxy
Deploy vProxy
Asset
Asset Assign Network
PLC
Create PLC and select network

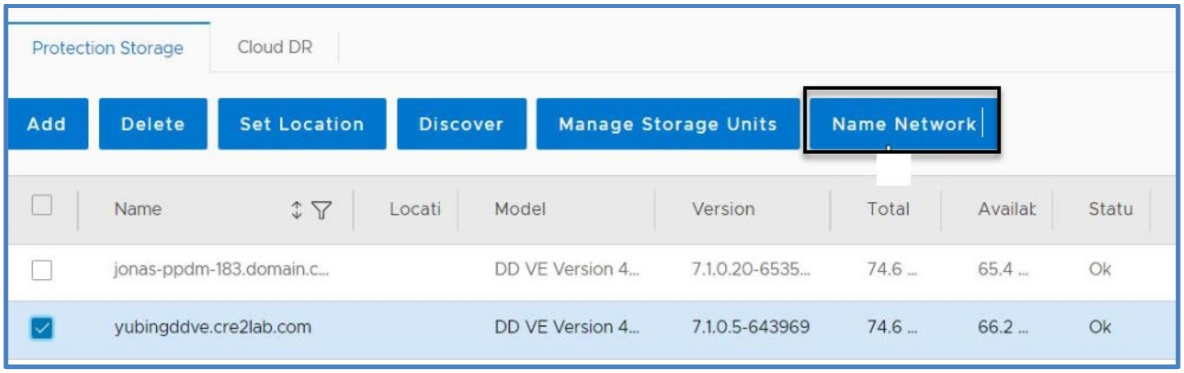
Figure 14. VLAN configuration steps

Discover and name PowerProtect DD series network or interface

After adding the DD series appliance as protection storage, name the virtual network between the PowerProtect Data Manager and the DD series appliance.

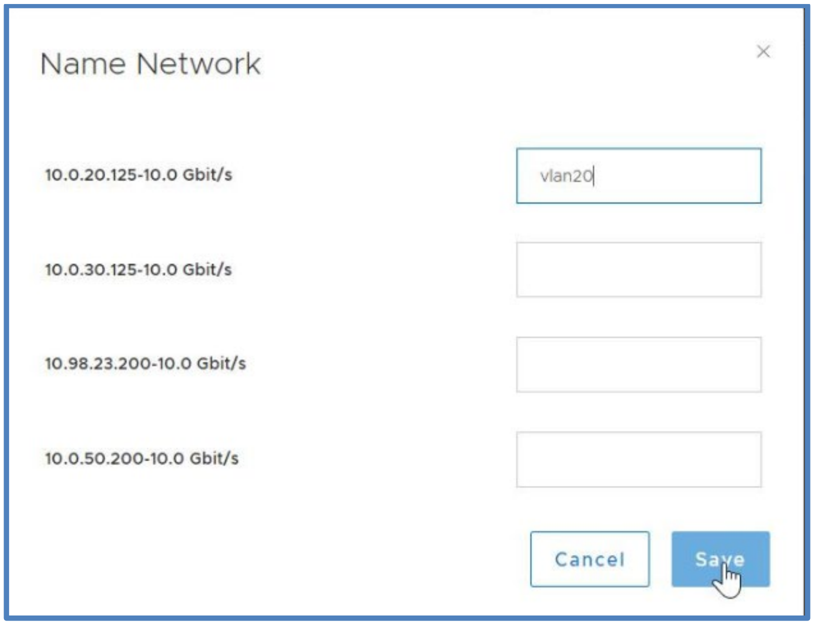
To rename a virtual network (edit the network name):

1. Select **Infrastructure** > **Storage** > **Protection Storage** and select the **Name Network** tab.



□	Name	Locati	Model	Version	Total	Availak	Statu
□	jonas-ppdm-183.domain.c...		DD VE Version 4...	7.1.0.20-6535...	74.6 ...	65.4 ...	Ok
☑	yubingddve.cre2lab.com		DD VE Version 4...	7.1.0.5-643969	74.6 ...	66.2 ...	Ok

2. Select the network, add the VLAN name, and click **Save**.

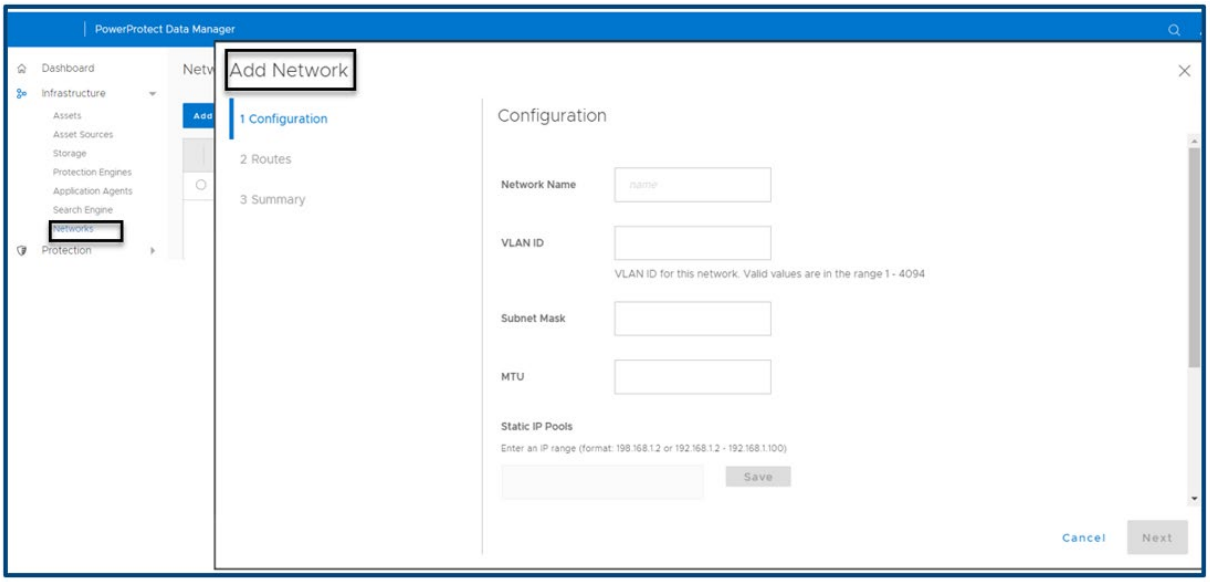


10.0.20.125-10.0 Gbit/s	vlan20
10.0.30.125-10.0 Gbit/s	
10.98.23.200-10.0 Gbit/s	
10.0.50.200-10.0 Gbit/s	

Add the virtual network to the PowerProtect Data Manager

Configure a new virtual network for use with assets and protection policies. Each new virtual network requires at least one IP address for a PowerProtect Data Manager network interface. Review the number of IP addresses needed field before you supply the required static IP addresses.

Select **Infrastructure** > **Networks** and click **Add Network**.



Configuration

Network Name: name

VLAN ID:

VLAN ID for this network. Valid values are in the range 1 - 4094

Subnet Mask:

MTU:

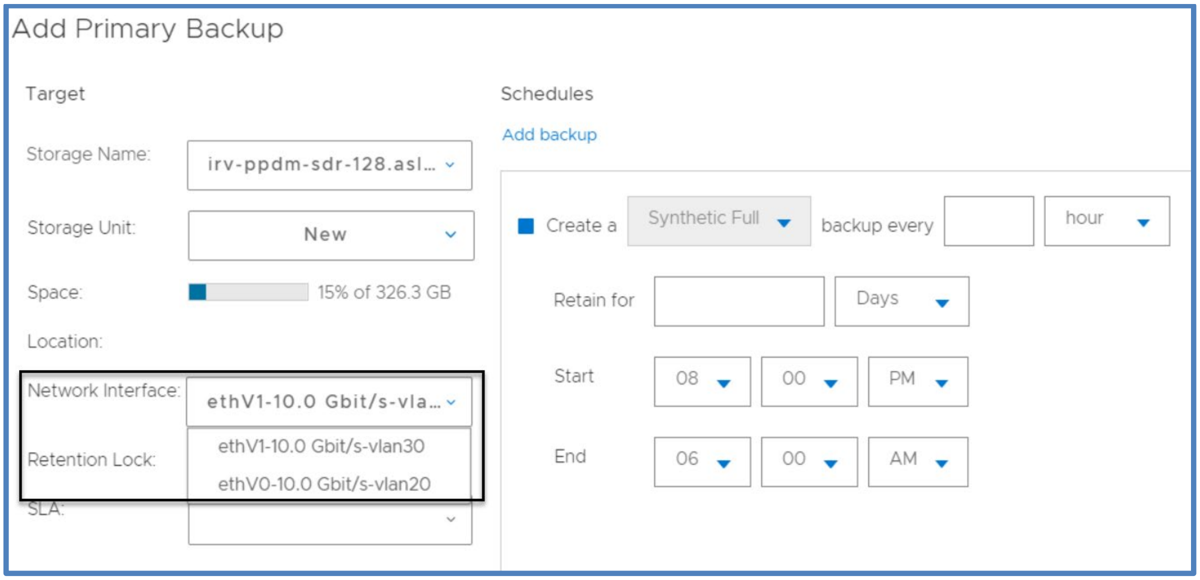
Static IP Pools

Enter an IP range (format: 198.168.1.2 or 192.168.1.2 - 192.168.1.100)

Assign the preferred virtual network to a protection policy or asset

Assignments identify which assets should use each virtual network. You can associate an asset with a virtual network by using one of two methods:

- **Using protection policy**: PowerProtect Data Manager can be configured to choose a preferred virtual network for all assets on a protection policy. The network interface has a drop-down menu, and you can select the preferred network for Primary backup and Replicate.



Storage Name: irv-ppdm-sdr-128.asl...

Storage Unit: New

Space: 15% of 326.3 GB

Location:

Network Interface: ethV1-10.0 Gbit/s-vla...

Retention Lock:

SLA:

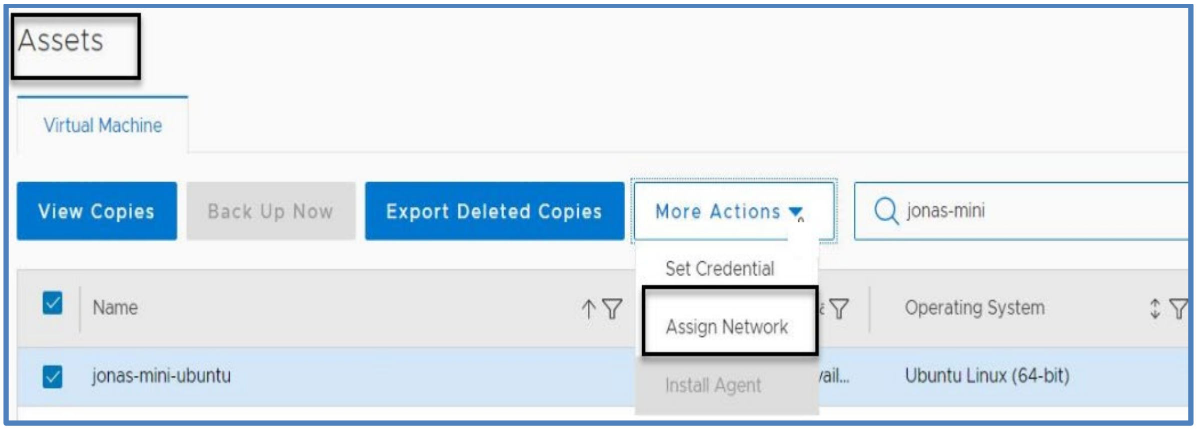
■ Create a Synthetic Full backup every hour

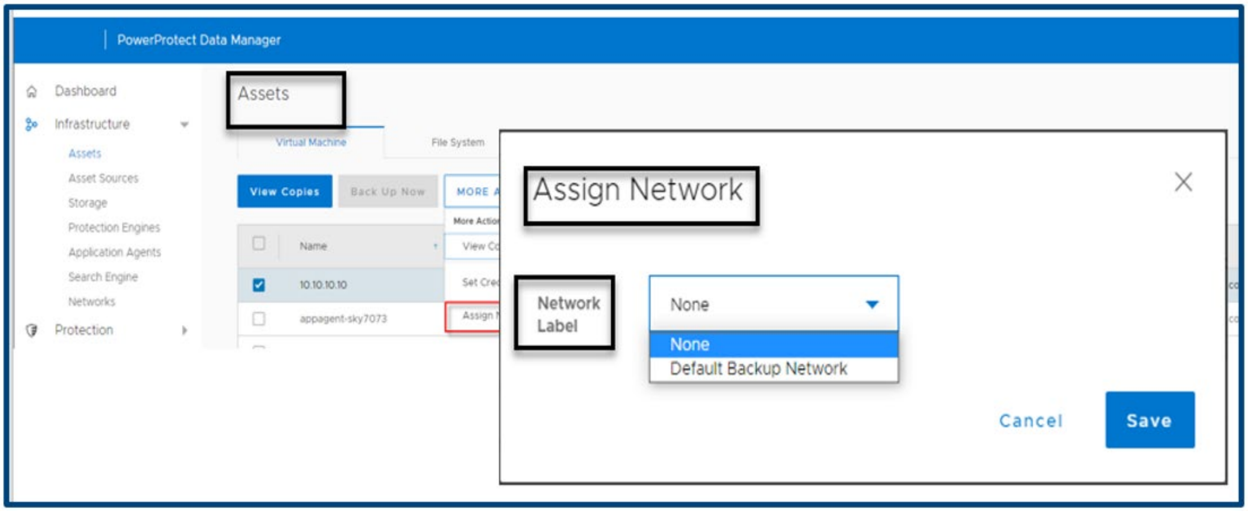
Retain for Days

Start 08 00 PM

End 06 00 AM

- **Using asset**: Virtual networks can be assigned to individual assets. This method is optional and overrides any virtual network assignment from a protection policy. Assets that are not individually assigned a virtual network automatically use the preferred virtual network.





Supported scenarios

PowerProtect Data Manager 19.11 supports virtual networks for the following use cases:

- Virtual machine backups
- Database backups
- Exchange backups
- File system backups
- Replication
- Disaster recovery
- Cloud DR
- Storage data management

Notes and limitations of multiple VLANs

Consider the following information when you are using multiple VLANs:

- PowerProtect Data Manager supports only VGT mode (multi VLAN) unlike vProxy, which supports both VST (single VLAN) and VGT modes. Therefore, the UI does not show a selection for a port group for PowerProtect Data Manager.
- No restrictions apply to the operation flow sequence. Any parameter can be edited to modify or add values for the defined parameters.

- The DD series appliance network name can be different, but PowerProtect Data Manager and assets must reach the DD series appliance network. Using a proper naming convention helps.
- Customers are responsible for ensuring that networks are reachable and configured correctly.
- An old vProxy cannot be edited and attached to a VST or VGT port group. It must be reconfigured.
- We recommend that you have PowerProtect Data Manager and the DD series appliance in the same VLAN; otherwise, proper gateway/routing must be established.
- Search can only be done in the default VLAN.
- PowerProtect Data Manager asset restriction (application and file system): If the assets of the same host/client are attached to different networks, those assets must be on different policy.

Scalability limits for PowerProtect Data Manager

The following limits have been tested successfully with PowerProtect Data Manager for the vCenter Server, the VM Direct Engine, and DD systems.

Table 7. Tested limits for PowerProtect Data Manager components

Component (per PowerProtect Data Manager)	Tested limits
vCenter Servers supported	12
External VM Direct Engines supported	40
DD series appliances supported	10
Virtual machines	10,000
Maximum search engine node	5

Notes:

These numbers are not maximum (hard) limits but should be considered as best practice when scaling your environment.

The vCenter server limit is subject to the VM Direct Engines overall limit of 40 and per vCenter limit of 25. For example, using the maximum tested number of vCenter servers (12), you could add an average of three VM Direct Engines per vCenter.

The number of external VM Direct Engines was tested across 10 vCenter servers (for example, 4 VM Direct Engines per vCenter).

Conclusion

This document provides a detailed overview of the PowerProtect Data Manager deployment requirements, process, and best practices to successfully deploy a new PowerProtect Data Manager.

Technical support and resources

Technical support

For the most up-to-date software compatibility information for PowerProtect Data Manager, see the E-Lab Navigator at https://elabnavigator.emc.com/eln/modernHomeDataProtection.

For technical support, see the Dell Support website.

Dell Technologies documentation

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

- PowerProtect Data Manager Info Hub
- PowerProtect Data Manager Administration and User Guide
- PowerProtect Data Manager Deployment Guide
- PowerProtect Data Manager Security Configuration Guide
- PowerProtect and Data Domain core documents