DELL Technologies

Technical White paper

Dell EMC PowerProtect Data Manager: Deployment Best Practice

Abstract

This white paper explains PowerProtect Data Manager deployment best practices. It discusses deployment requirements and the setup of a new PowerProtect Data Manager.

July 2021

Revisions

Date	Description
July 2019	Initial release
October 2020	Revision
July 2021	Revision

Acknowledgments

Author: Sonali Dwivedi

Co-Author: Debjeet Bagchi and Richard Forshaw

Table of contents

Executive summary

Data protection has become an integral and essential part of any successful business. The need to provide a powerful, scalable, and yet 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 the Mid-Market industry demands Dell EMC has come up with a new offering called PowerProtect Data Manager.

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.

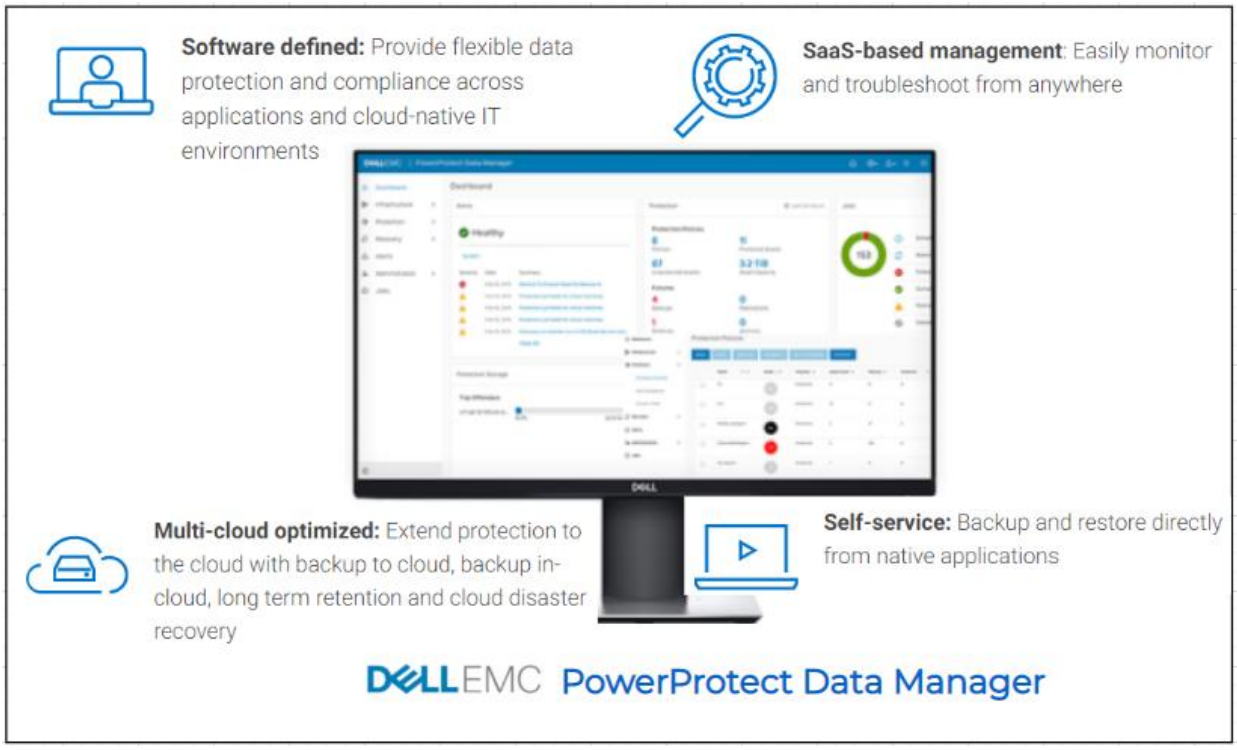
This white paper is focused on the PowerProtect Data Manager deployment requirements and best practices.

Audience

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

1 PowerProtect Data Manager Overview

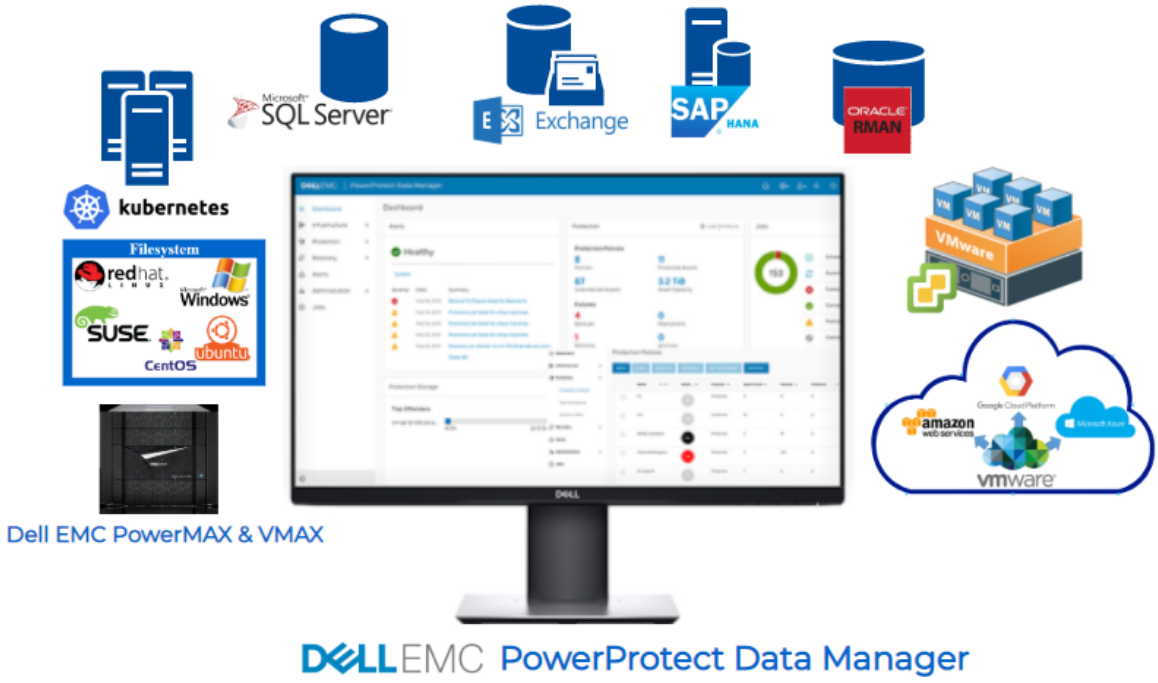
Data Manager integrates multiple data protection products within the Dell EMC Data Protection portfolio to enable data protection as a service. Data Manager enables new data paths with provisioning, automation, and scheduling that enable a data protection team to embed protection engines into their infrastructure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



Data Manager integrates multiple data protection products within the Dell EMC Data Protection portfolio to enable data protection as a service, providing the following benefits:

- Enables the data protection team to create data paths with provisioning, automation, and scheduling to embed protection engines into the infrastructure for high-performance backup and recovery.
- 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 Data Manager server:
  - VMware Virtual Machines
  - File Systems
  - VMAX Storage Groups
  - Kubernetes clusters
  - Microsoft Exchange and SQL databases
  - Oracle databases
  - SAP HANA databases
- To get the details on the version support and compatibility check *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.

2 PowerProtect Data Manager Deployment Methods

You can deploy 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 Data Manager after its deployment.

2.1 OVA deployments

Considerations of OVA deployments include the following:

- Data Manager can be deployed to on-premises virtual hosts or to cloud-based environments that include VMware Cloud on Dell EMC, VMware Cloud (VMC) on Amazon Web Services (AWS), and Azure VMware Solution (AVS) on Microsoft Azure.
- OVAs are deployed using the vSphere Client.
- Deployed 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.
- Data Manager and DDVE cannot be deployed simultaneously from the same interface.

2.2 Machine-image deployments

Considerations of machine-image deployments include the following:

- 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 Data Manager can still protect resources in those environments.
- Machine images are deployed using the web-based user interface of a cloud provider.
- Deployed Data Manager instances detect their environment and are automatically appropriately configured.
- Data Manager and DDVE can be deployed simultaneously and from the same interface.

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

- *PowerProtect Data Manager AWS Deployment Guide*
- *PowerProtect Data Manager Azure Deployment Guide*
- *PowerProtect Data Manager GCP Deployment Guide*

3 PowerProtect Data Manager Deployment Considerations

Planning the environment for deploying Data Manager using OVA plays an important pre-requisite function. It is necessary to facilitate adequate resources to achieve optimal performance of the Data Manager.

3.1 Planning VMware vCenter Resources

1. PowerProtect Data Manager Appliance

The minimum resource requirements to deploy a Data Manager OVA in VMware vSphere 6.0 and above are:

Specification	Value
CPU	10 CPU cores
Memory	18 GB RAM
Disk	Disk 1 - 100 GB Disk 2 - 500 GB Disk 3 and 4 – 10 GB each Disk 5 through 7 – 7 GB each
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 later VMware ESXi server version 6.5 or later VMware tool version 10.1 and later
For Cloud DR	14 CPU cores (10 for Data Manager and 4 for Cloud DR) 22 GB RAM (18 GB for Data Manager and 4 GB for Cloud DR)

2. PowerProtect Search Engine

The PowerProtect Search 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 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 below system requirements:

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 Data Manager. One search node can index maximum 1 billion files or 1000 virtual machines.

3. PowerProtect VM Direct Protection Engine

Data Manager comes pre-bundled with an embedded VM Direct engine which 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 external protection engine also known as a VM proxy, because the embedded proxy has limited capacity for performing parallel backups.

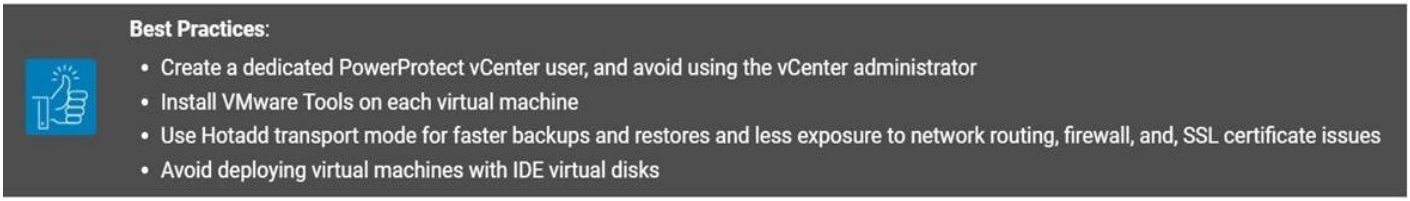
The following details the requirements for the external VM Direct Engine:

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)

Note:

- Total number of external VM Direct engines supported with a single vCenter server is 25, although the recommended number is 7.
- Network setting like 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.
- Embedded VM Direct Engine supports 4 backup and restore sessions.



3.2 Planning the Protection Storage

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

The 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 is the supported version of DD series appliance:

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

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

For more details check on DD Management Center Release Notes.

3.3 Planning Networking

Following are the networking requirements for deploying Data Manager:

1. IP and DNS requirement

Following are the requirements for networking:

- Unique IP address must be allocated to the Data Manager, VM Search Engine and VM Direct Engine. Only IPV4 IP addresses are supported.
- NTP servers are recommended to sync 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 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 fails if the Data Manager server is deployed in the same private network as the internal Docker network.

2. Firewall and Port Requirements

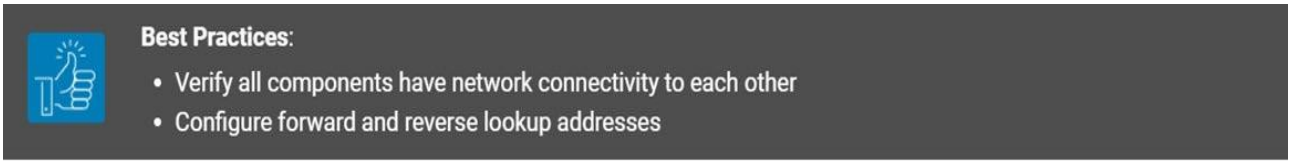
Data Manager is a single node in a virtual appliance that uses the Linux SLES 12 firewall to protect and limit external access to the system. Data Manager uses a direct socket connection to communicate and move data internally and across the network to the required service with minimal overhead.

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

Description	Communication	Port
SSH communications	Bi-directional communication between the SSH client and the Data Manager appliance	22 TCP/UDP
SQL, Oracle, Exchange, SAP HANA, File System	Bi-directional communication between the Data Manager agent and the Data Manager appliance. Requirement applies to Application Direct and VM Direct.	7000 TCP
REST Server	Bi-directional communication between the HTTP client and the Data Manager appliance.	8443 TCP

RESTAPI Server – VM Direct	Bi-directional communication between the Data Manager agent and the 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 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 Data Manager appliance. This requirement applies to both Application Direct and VM Direct.	7000 TCP
Embedded VM Direct service	Outbound	9090 TCP
PowerProtect Controller	Outbound between the Data Manager appliance and PowerProtect Controller on the Kubernetes cluster. This port is used by the Data Manager 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 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, check PowerProtect Data Manager Security Configuration Guide.



3.4 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

3.5 User permission requirements for supported platforms

Following table shows a quick overview of the permissions requirements for all supported platforms.

Note: Check individual guides for detailed overview of permissions for each workload.

Application Workload	Installation and Discovery	Backup		Recovery	Documentation (For details)
		Self-Service	Centralized		
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	NA	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 admin, catalog read role. **Tenant database:** Either system database user with database admin role or tenant database admin with Backup admin, Catalog read roles.	**HANA studio:** System database: System database user with Backup admin, catalog read role. Tenant database: Either system database user with database admin role or tenant database admin with Backup admin,	Database admin user or Hana <sid>adm operating system user	*PowerProtect Data Manager SAP HANA Agent User Guide*

			Catalog read roles. **HANA CLI** Hana (<sid>adm) user from CLI		
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 onwards 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 onwards 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 onwards 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 Agent User Guide*
VMware	Create 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.	NA	Dedicated vCenter user account at the root level of vCenter. Note: Full permission list is mentioned in the guide under “Creating a dedicated vCenter user account”.	Full VM restore : Dedicated vCenter user account at the root level of vCenter. For FLR restore: Any user with local administrator privileges	*PowerProtect Data Manager Administration and 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 admin role.	Ddboost and DdVdiskUser specified in the lockbox configuration file must have the admin role.	Ddboost and DdVdiskUser specified in the lockbox configuration file must have the admin role.	*PowerProtect Data Manager Storage Direct Agent User Guide*

Note: Following steps explain how to provide local admin privileges correctly to domain user on Windows server:

- On the Active Directory server, create domain user account (dns\domain user) or use an existing domain user.
- Make the user member of “Backup Operations” and “Remote Desktop Users”.
- Log in to application host as system administrator.
- Go to Control Panel -> User Accounts -> Manage User Accounts -> Add the new user here with local admin privileges.
- Click Start -> Administrative Tools -> Local Security Policy -> User Rights Assignment -> Log on as a Service -> Add the new user.
- Disable UAC
- This domain user account can now be used to do SQL, Exchange, and File System application agent installation.

3.6 Planning License

The available license types are as follows.

- Trial—applied automatically on installation of Data Manager and enabling full use of the product for up to 90 days without applying a license key. When the trial period ends, 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 (SupportAssist replaces Secure Remote Services (SRS) in 19.8 release of Data Manager) connections are removed from the system and replaced with a 90-day trial license. Therefore a valid FETB license for Data Manager and any associated Secure Remote Services connections must be reinstalled.

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

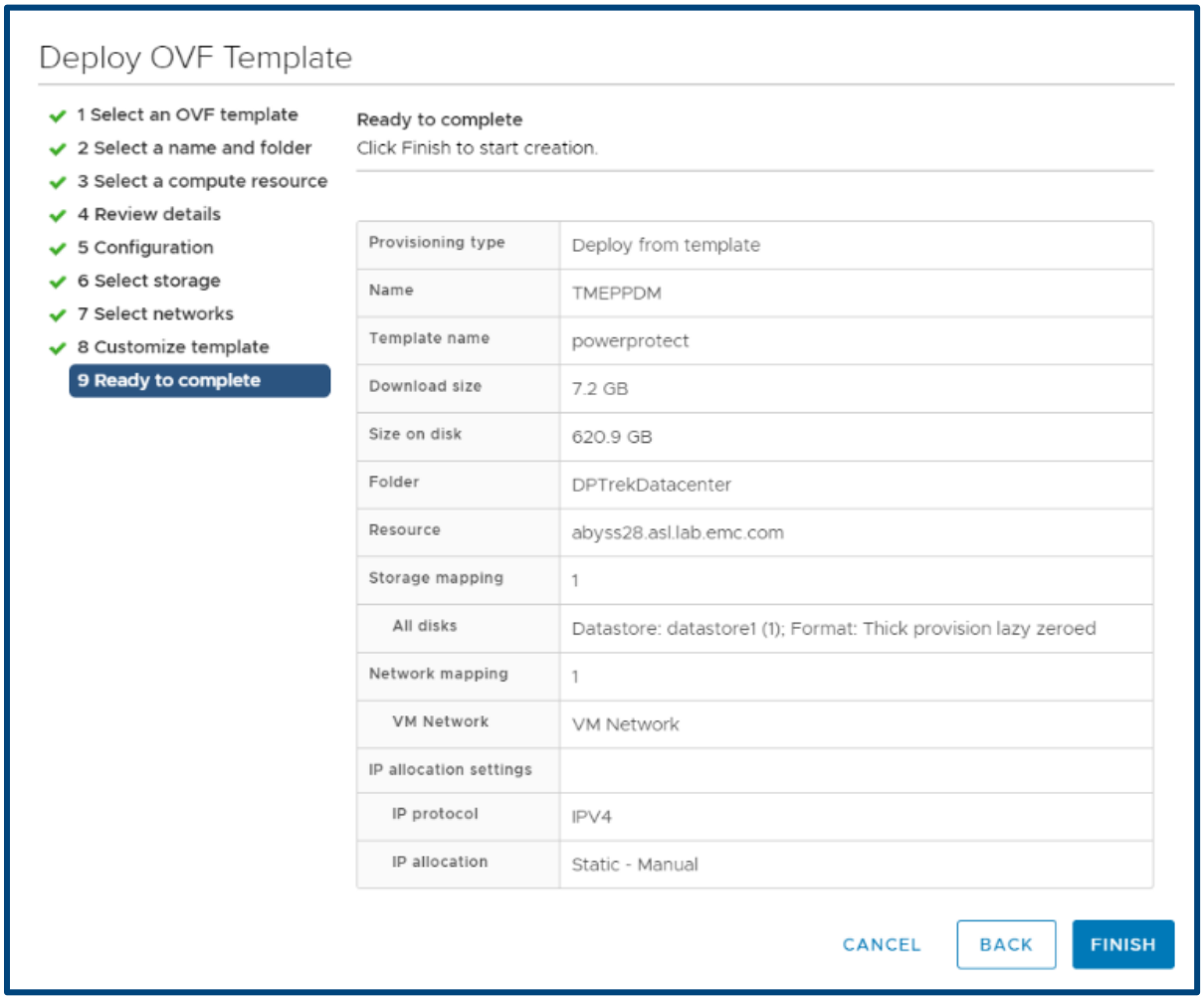
4 Deployment of PowerProtect Data Manager

Data Manager Appliance is easy to install and configure. The 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 Data Manager OVA deployment is completed all the services and components of the software are accessible.



5 Post Installation steps for PowerProtect Data Manager

Once the Data Manager OVA is successfully deployed and the VM is powered ON, the PowerProtect Data Manager UI can be accessed by entering the IP address or FQDN configured during the deployment using **https://*appliance_hostname.***

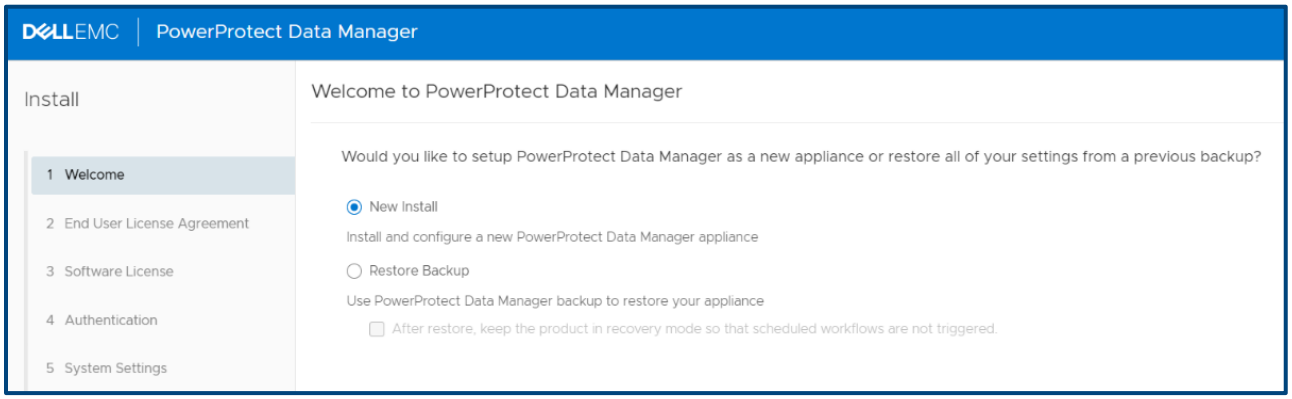
The security certificate that encrypts communication between the Data Manager UI and the web browser is self-signed. A self-signed certificate has been signed by the web server that hosts the secure web page being viewed by a web browser. This certificate is enough to establish an encrypted channel between 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 Data Manager. Google Chrome is the only supported browser.

5.1 Login Screen

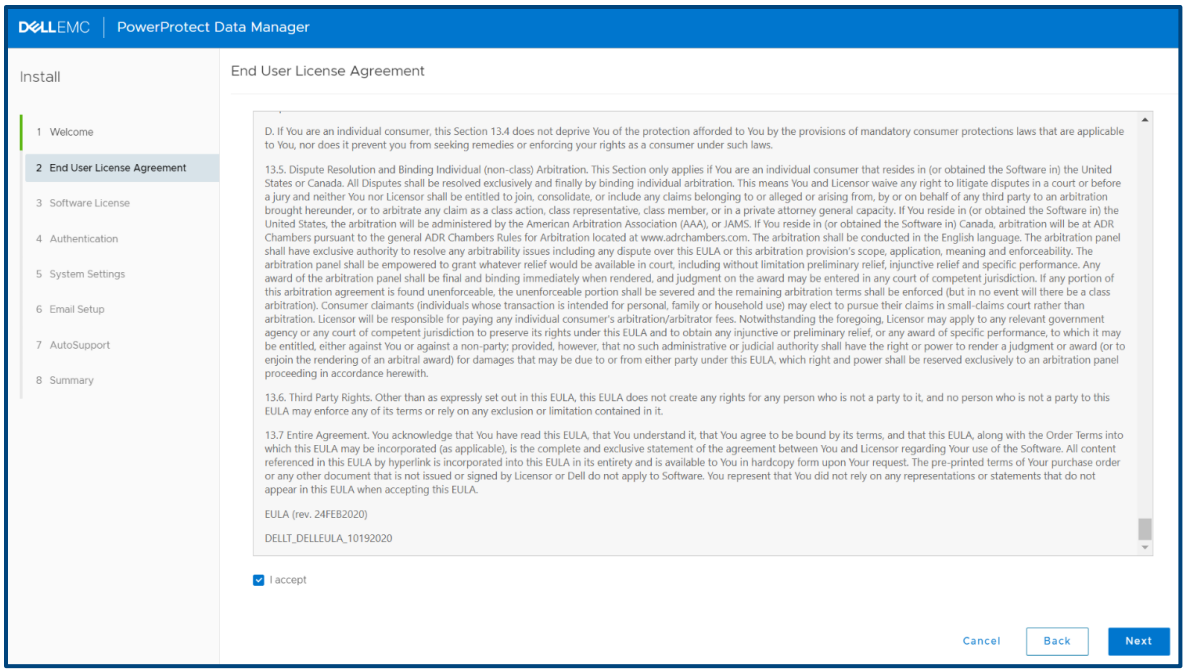
The Welcome screen is displayed when the PowerProtect UI is accessed for the first time after deploying the OVF template. There are two options available on this screen: New Install and Restore Backup.

- New Install -If you are installing the device first time then select New Install.
- Restore Backup – This option is used when 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 Data Manager.



5.2 End-user license agreement (EULA)

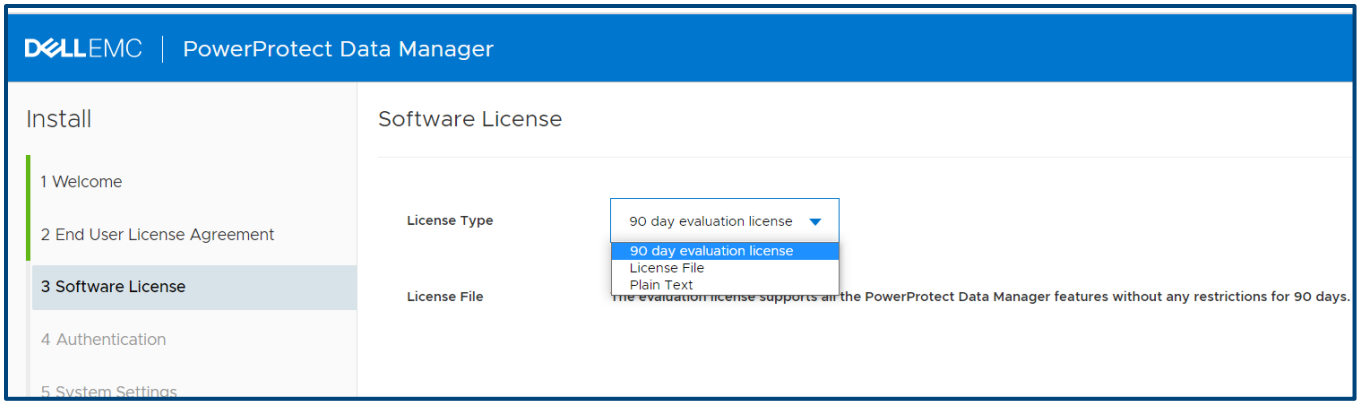
Scroll through the agreement and accept the license.



5.3 License

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 EMC license management website. To obtain the license file, you must have the License Authorization Code (LAC), which Modifying the System Settings was emailed from Dell EMC. If you have not received the LAC, contact your technical support representative.



5.4 Authentication

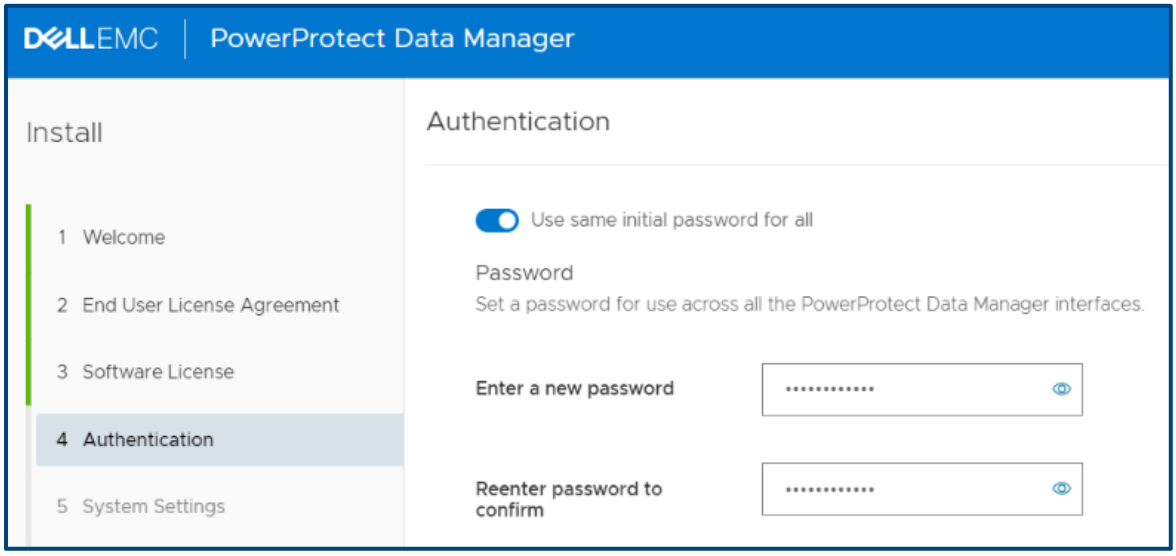
The authentication screen allows the Administrator to set an authentication password for various users with different roles. Users can be defined as either local or LDAP/Active Directory. Users and LDAP groups can access all protection policies and assets within the Data Manager environment.

From the Data Manager CLI, password expiry can be set to ‘never’ for users such as admin, root, and support accounts using the following command:

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

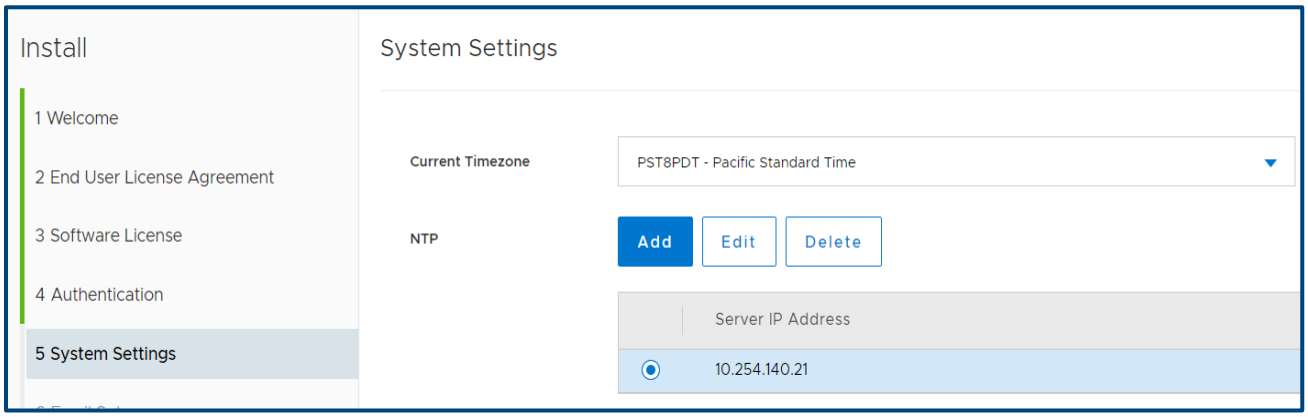
- Admin password is used to log in to the Data Manager management console.
- Service password is used to log in to ssh for support activities.
- Lockbox password is used during restore operations.

Note: The **Use of the same password for all** checkbox can be selected to set the same password for admin, service, and lockbox accounts but it is not recommended. It is advised to save all the passwords securely for later use.



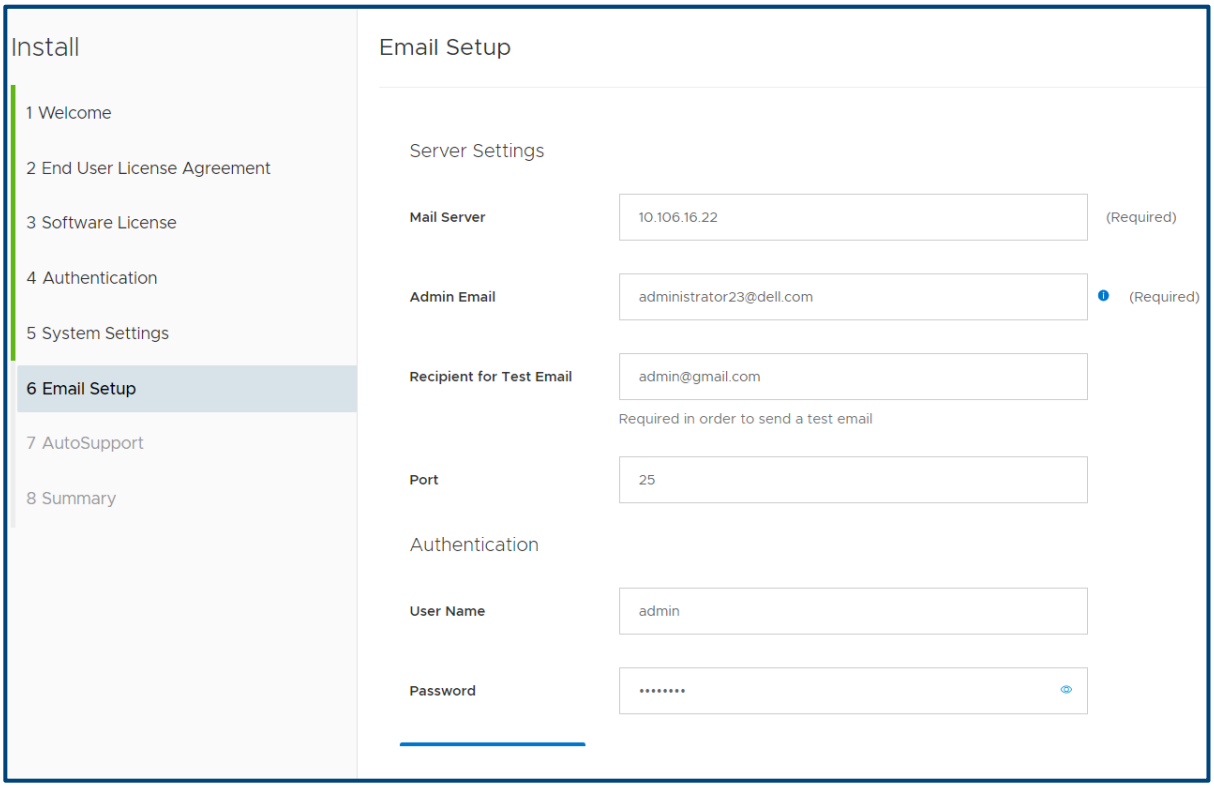
5.5 System Settings

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



5.6 Email and SMTP setup

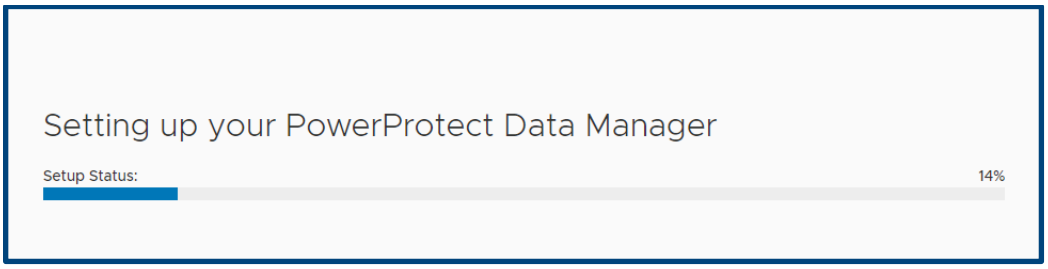
Email setup is an optional step. The SMTP server can be configured to receive the Data Manager alerts using a specified email address. To send diagnostic and usage data to Dell EMC for proactive support and to help improve our products and services, switch Auto Support to ON.

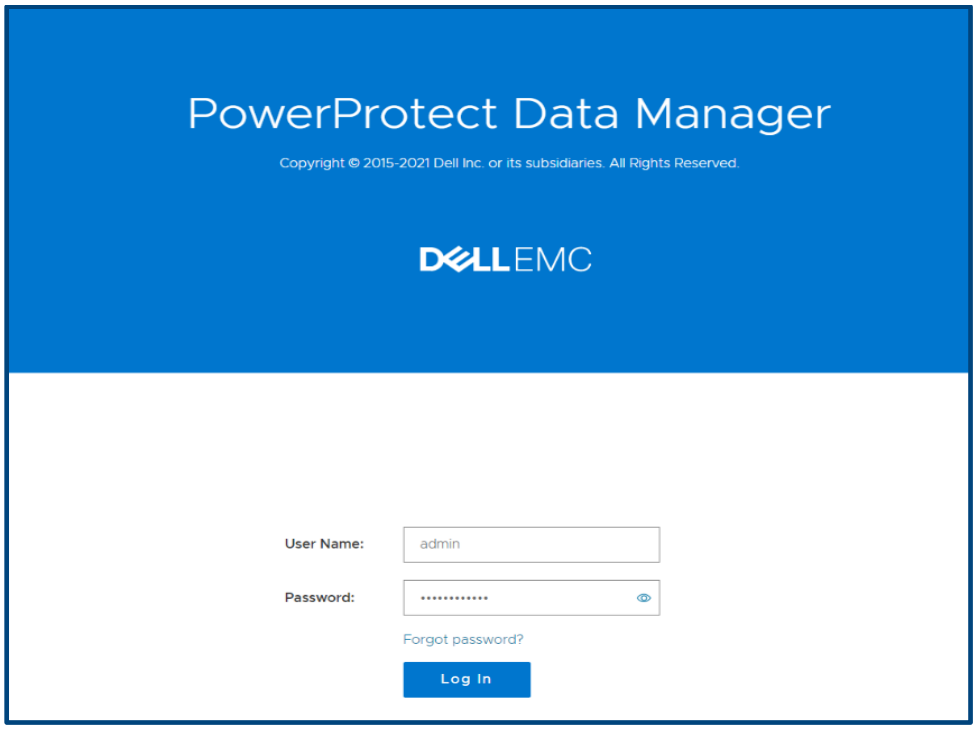


5.7 Login and Getting Started

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

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



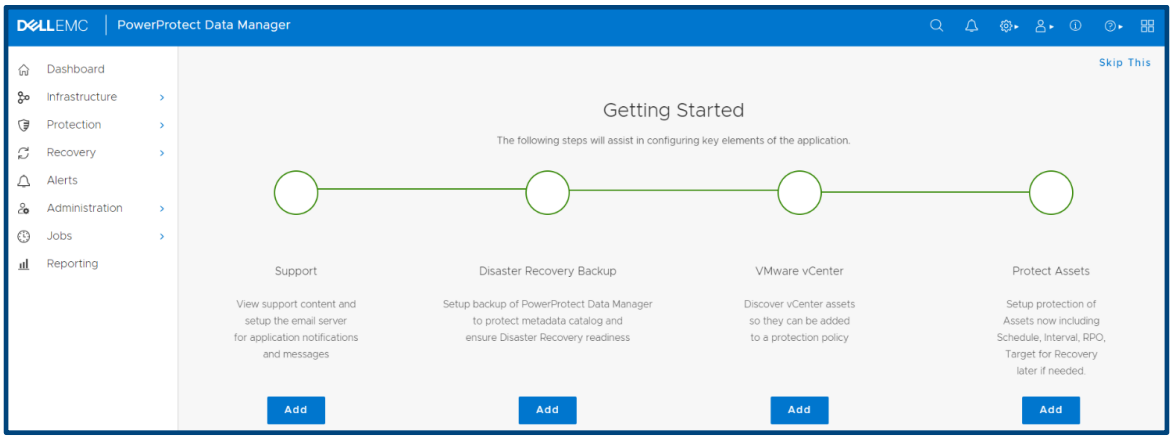


After logging in, the “Getting Started” screen is visible. The Data Manager navigates back to Get Started until you exit Getting Started. To exit Getting Started, click **Skip This**.

Getting Started can be accessed anytime through System Settings > Getting Started.

There are four navigation options from the Getting Started screen, which are:

- Support - links to the SupportAssist configuration page.
- Disaster Recovery Backup - links to the appliance backup configuration workflow.
- VMware vCenter - links to the workflow to add vCenter as asset sources.
- Protect Assets - links to the Protection Life-Cycle workflow for all asset types.



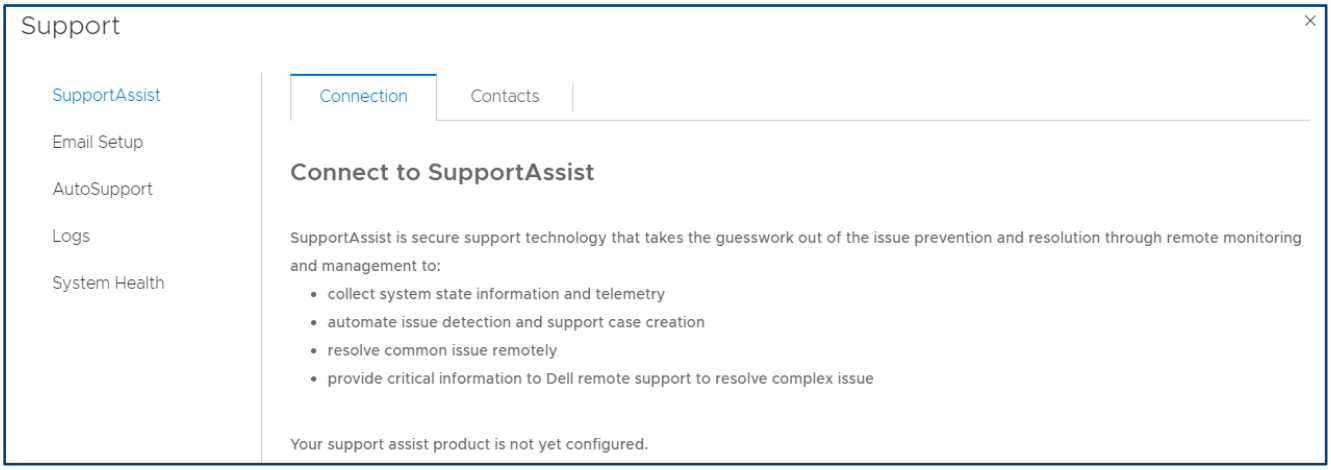
5.8 Configure SupportAssist for PowerProtect Data Manager

SupportAssist is a support tool that communicates with 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 Data Manager systems. SupportAssist replaces Secure Remote Services (SRS) in the current release of Data Manager. If you have configured SRS previously, the Data Manager system automatically migrates SRS to SupportAssist when you upgrade the Data Manager.



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

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

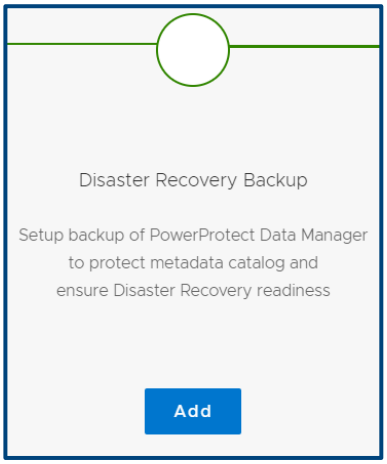
5.9 Setting up disaster recovery of PowerProtect Data Manager

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

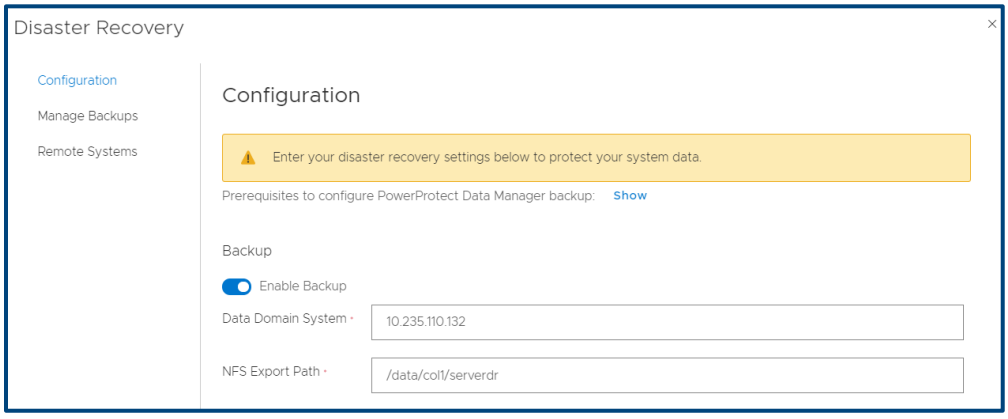
- Each backup is considered a “full” backup although it is created in an incremental manner. The persistent data that is saved in a backup includes the Lockbox and Elasticsearch databases.
- The backup operation creates a Point-in-Time snapshot of the database while the system is in a quiesced state. While the system is quiesced, user functionality is limited. After the snapshot completes, and while

Data Manager copies the snapshots to the DD storage unit, full user functionality is restored. If the system fails to quiesce, Data Manager still takes a backup, which is marked as crash consistent instead of application consistent.

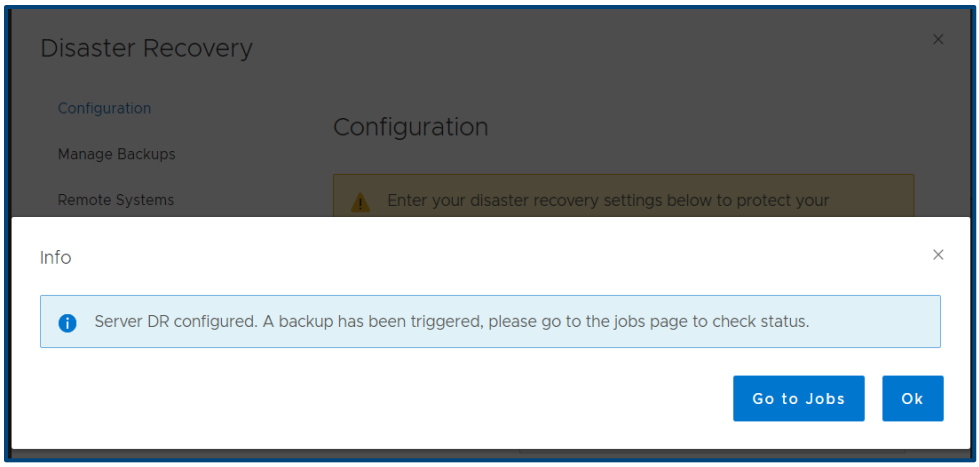
- To store system backups, you must configure and assign a private DD storage unit for the Data Manager system. The system protection service enables you to manage the frequency and start time of an automated system backup, perform manual backups, and define the length of time that the system backups are available for recovery.

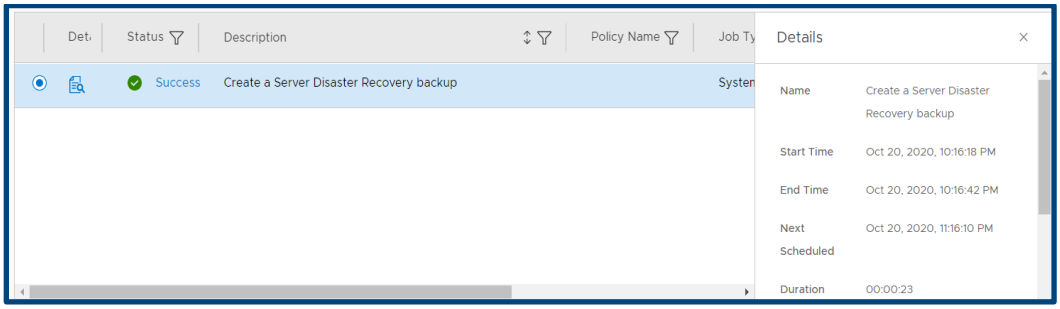


- File Search indexes are backed up for DR recovery along with other component DR backups. For this release, recovery requires manual steps. Contact Customer Support to assist with this requirement.
- Enter the following information, and then click Save.
  - Select Enable backup.
  - DD System—IP address or hostname of the DD series appliance where you created the MTree with NFS Export.
  - NFS Export Path—the path of the NFS Export (select show to get full instructions on creating NFS export on DD series appliance).



Result - the initial backup runs, and then backups are automatically triggered every hour.





5.10 Add asset sources

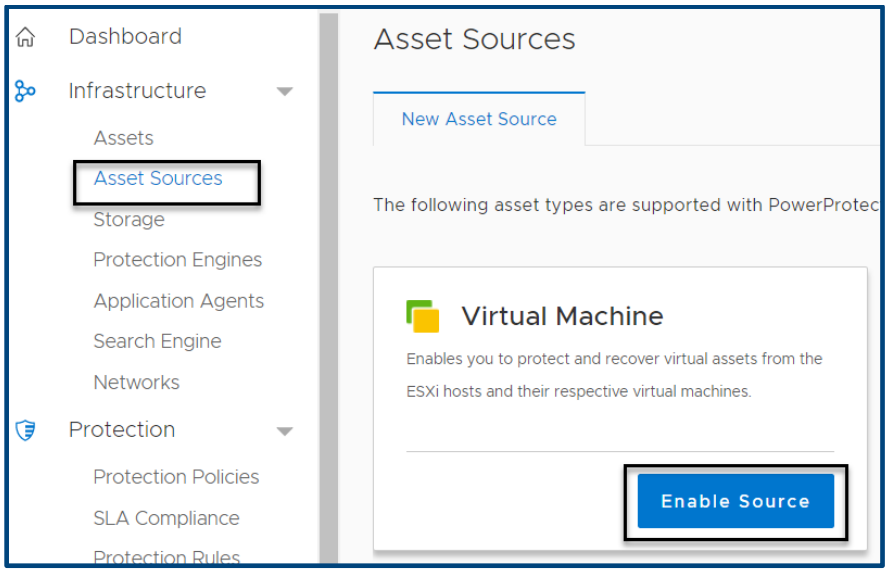
In Data Manager, assets are the basic units that Data Manager protects. Asset sources are the mechanism that Data Manager uses to manage assets and communicate with the storage system where backup copies of the assets are stored.

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.

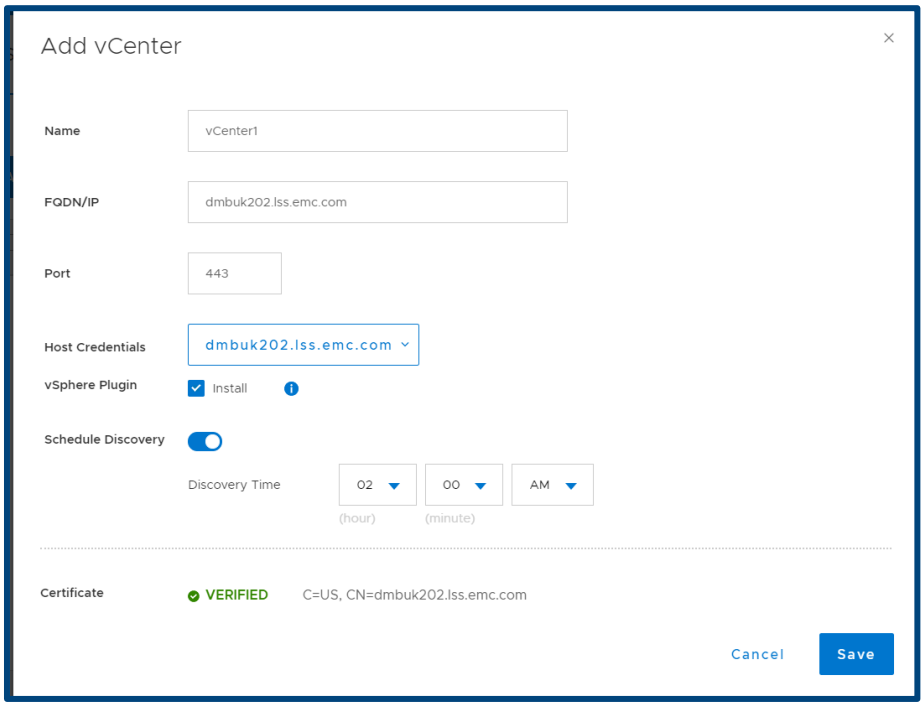
5.10.1 Add a vCenter Server

An asset source, such as a vCenter Server, must be enabled in Data Manager before you can add and register the asset source for the protection of assets. Perform the following steps to add a vCenter Server as an asset source in the Data Manager UI.

- Infrastructure → Asset Sources → Virtual Machine → Enable Source



Enter vCenter Details → Save



- The initial vCenter Server discovery identifies all 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.
- Upon successful discovery of the vCenter virtual machine assets, you can add a VM Direct appliance to facilitate data movement and then create virtual machine protection policies to back up these assets.

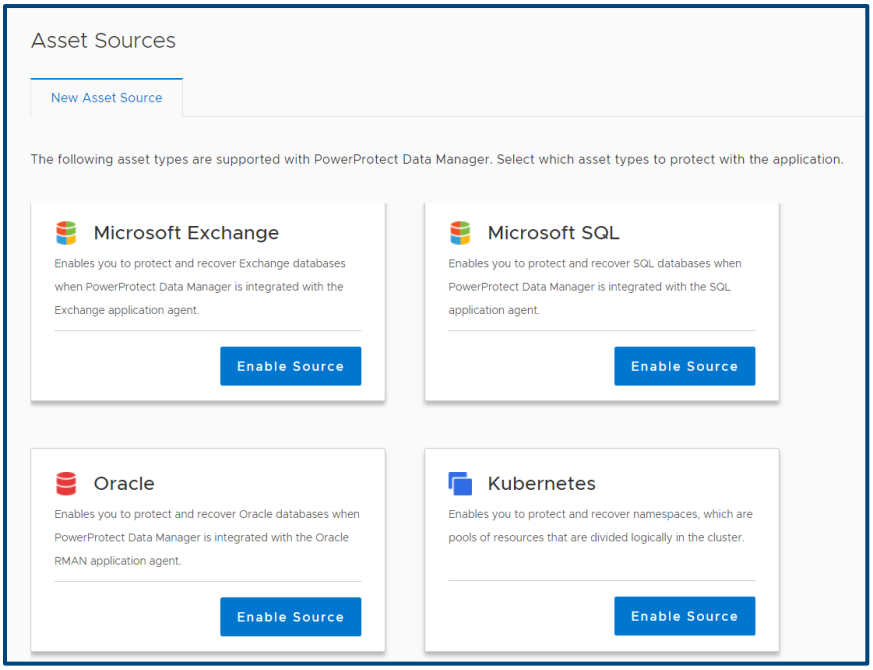
5.10.2 Add other asset sources

In addition to vCenter Server asset sources, Data Manager provides the option to enable the following asset sources to protect Application Agent 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. Check the individual application agent user guides linked under *User permission requirements for supported platforms* for more information.

Infrastructure → Asset Sources → Enable Source

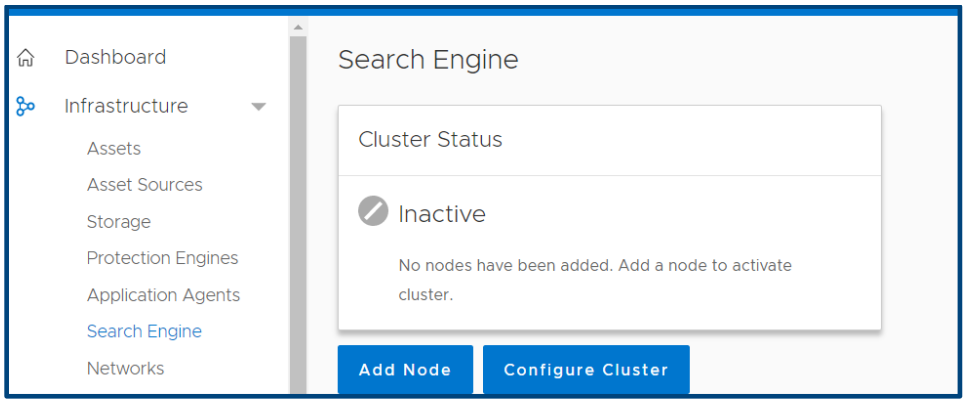


5.11 Configuring PowerProtect Search Engine

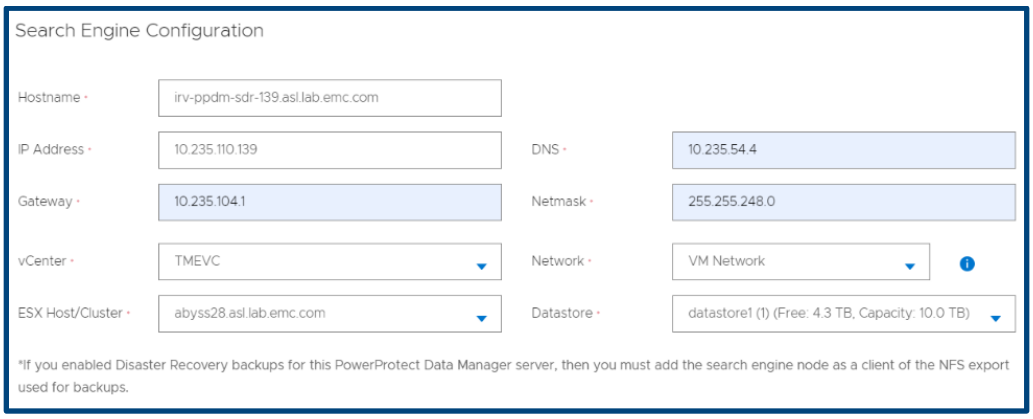
When you install Data Manager version 19.3 or later, the PowerProtect Search Engine is installed by default. The following bullet points explain its usage:

- 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.

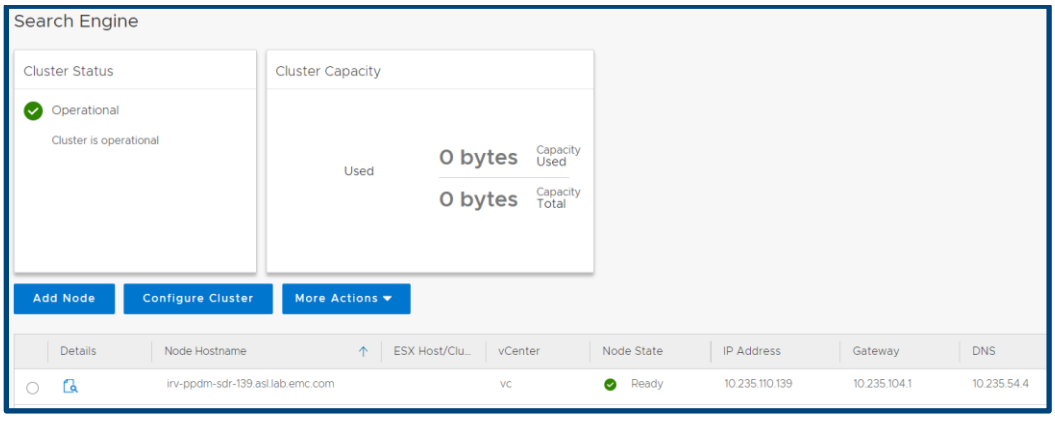
- PowerProtect Search is an optional feature that can be enabled, set up, and configured for virtual machine backups and protection policies. When you enable this feature, a backup of the Search Engine is taken as part of the server backup process.
- As of this release, you cannot disable these backups. When Search is enabled, you must white-list 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.
- To add Search Engine, Select Infrastructure → Search Engine → Add Node



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



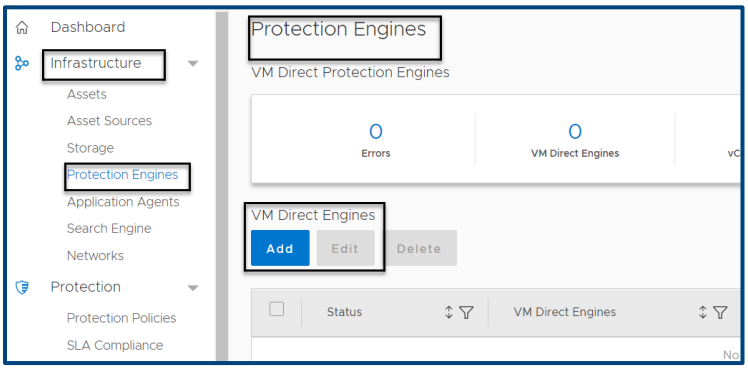
- Select Add and then wait few minutes for the VM to show node state ready.



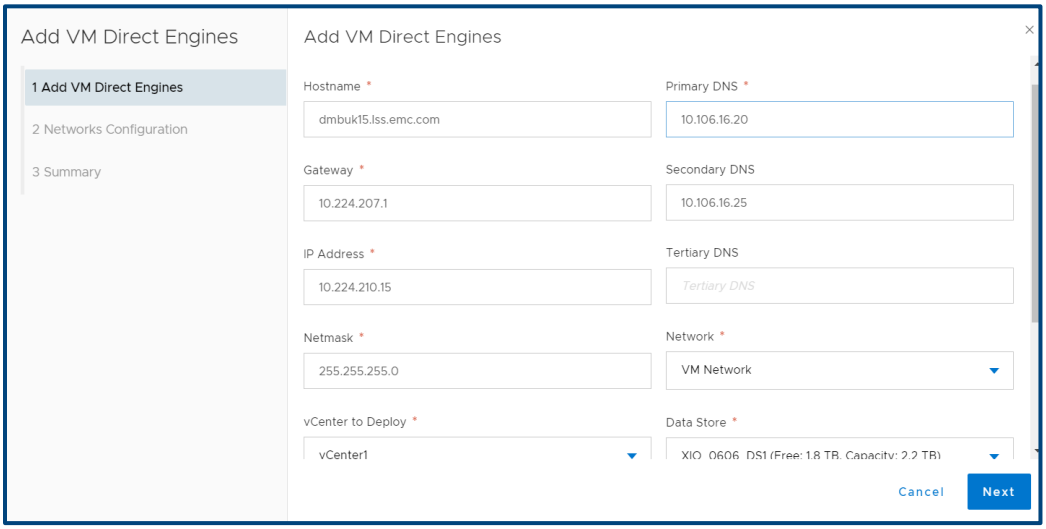
5.12 Adding External VM Direct Engine

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

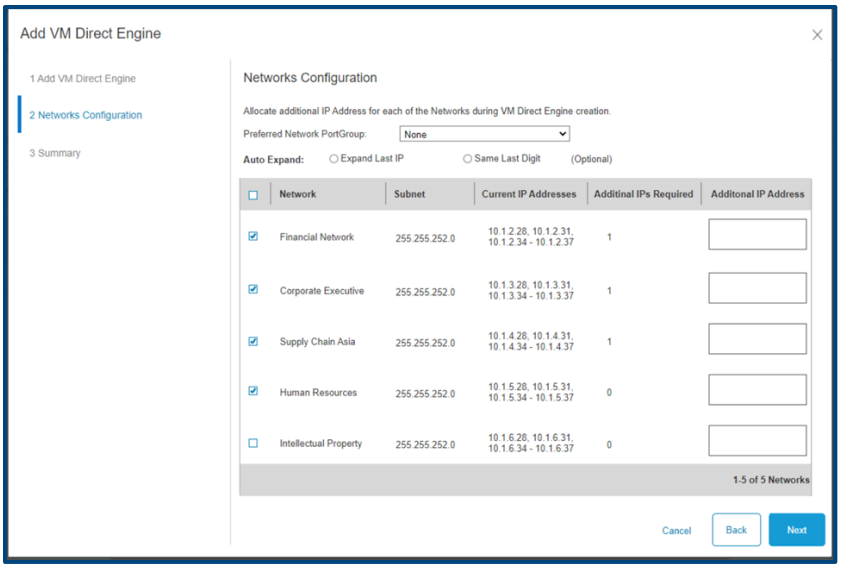
- Infrastructure → Protection Engine → Add



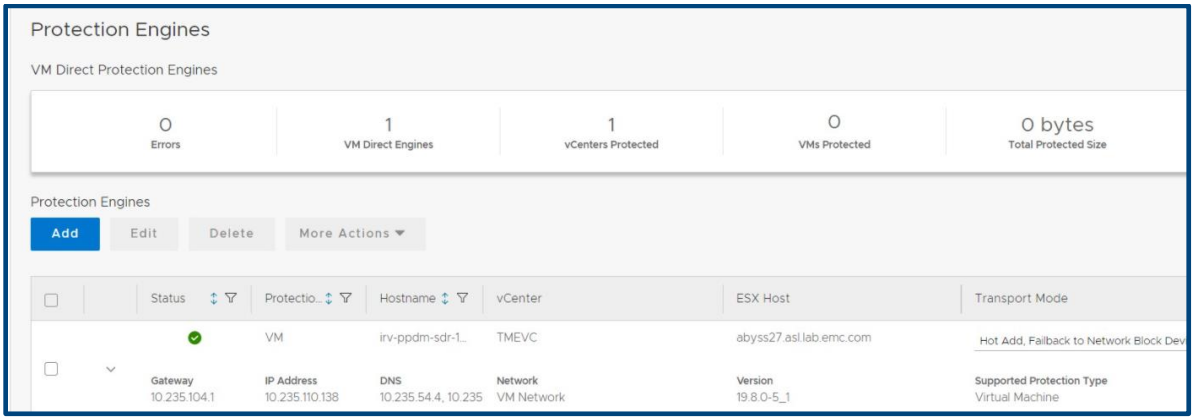
- Enter the network details and select Next.



- Select the VLAN network configured for the VM Direct Engine. To get more details on adding multiple VLANs check Multiple VLAN configurations section.



- The proxy is deployed on the vCenter automatically. Once its status shows that as ready then VM backups can be configured.



5.13 Adding PowerProtect DD Series Appliance

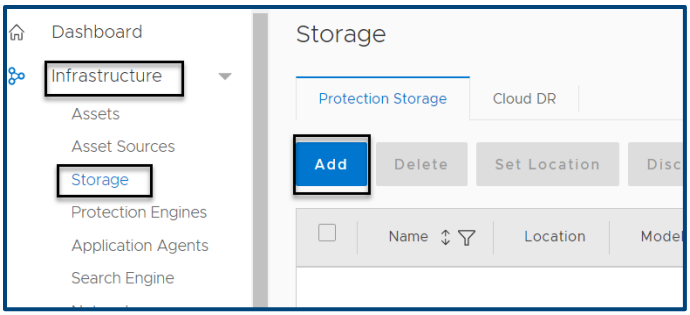
The PowerProtect Data Manager UI enables users with administrator credentials to add the following storage types:

- PowerProtect DD Management Center
- External PowerProtect DD series appliance

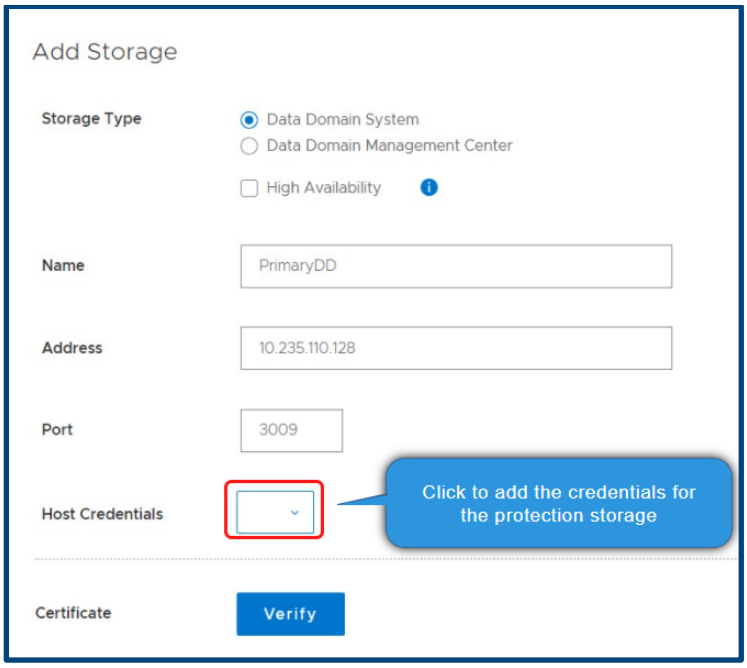
For each PowerProtect DD series appliance, the PowerProtect DD Management Center that manages the DD system is indicated in the Managed By column in the table.

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

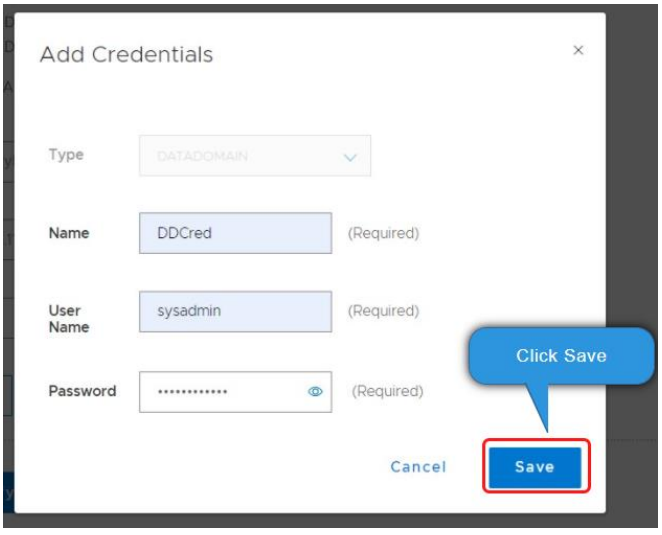
- Select Infrastructure → Storage → Add



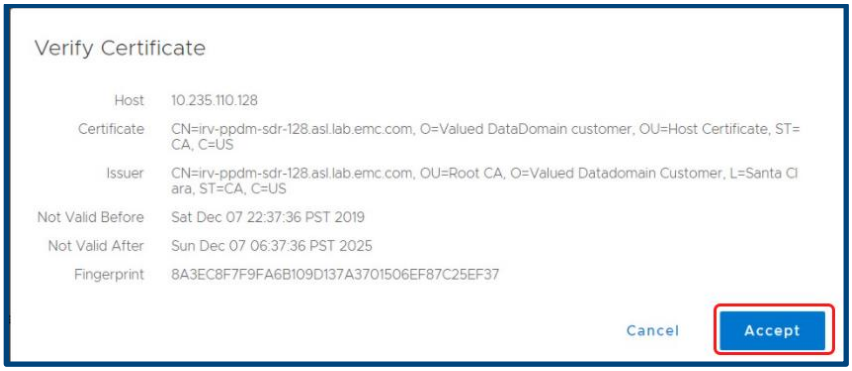
- Enter the DD series appliance details and Save.



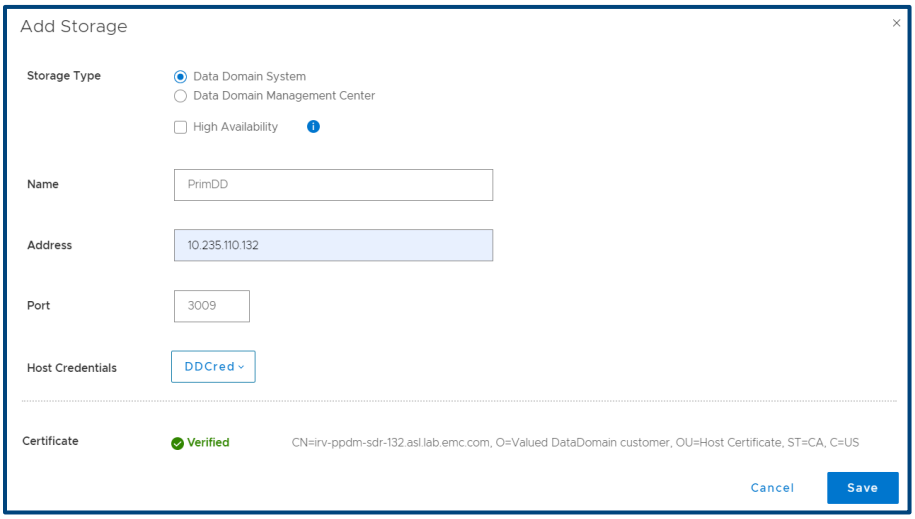
- Add Host credentials and click Save.



- Accept and verify the certificate .



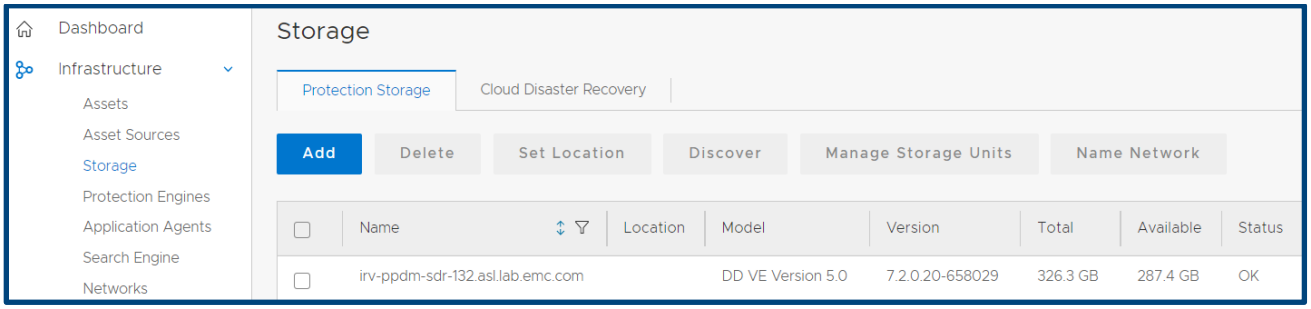
- Click Save after verified message is visible for certificate.



5.14 Verification

Verify that DD series appliance has been added to the Data Manager successfully.

Discovery should complete in a few minutes and will be under Infrastructure > Storage > Protection Storage tab.

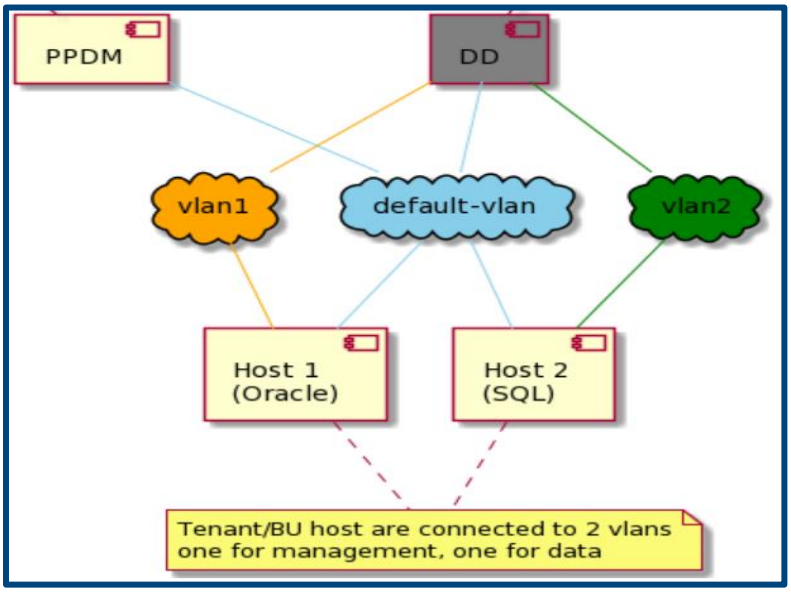


You are now ready to start configuring the backups. Check *PowerProtect Data Manager Administration Guide* for more information regarding configuring VM, File System and Application backups along with other management activities.

6 Multiple VLAN Configurations

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 segregate traffic that originates from different networks.



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

- Register the vCenter server on which the Data Manager is deployed. You can verify this on the vCenter tab of the Asset Sources page.
- Configure the network switch port for trunk mode. This setting allows the port to carry traffic for multiple VLANs.
- Enable Virtual Guest Tagging (VGT) mode on the VMware ESXi virtual network switch port for the Data Manager. Configure the virtual switch port for VLAN ID 4095.
- 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.
- Add the DD series appliance as protection storage for the Data Manager.

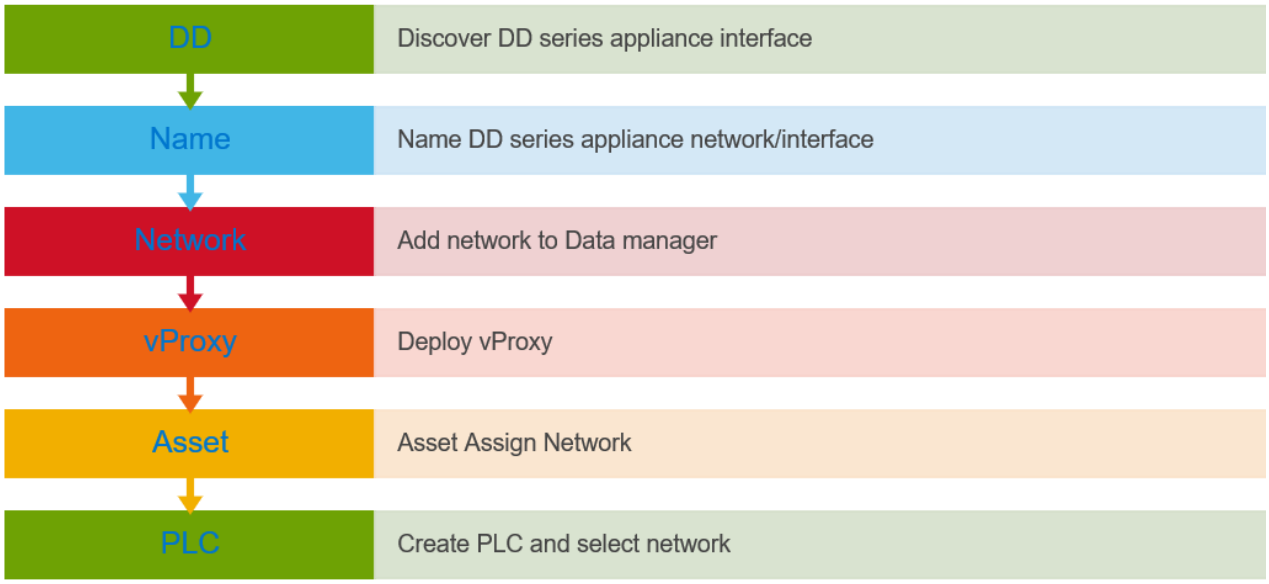
Note: Data Manager does not verify the network switch configurations. If the physical or virtual network switch is incorrectly configured, then virtual network configuration fails.

6.1 Steps to configure VLAN

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. 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 Data Manager user interface.

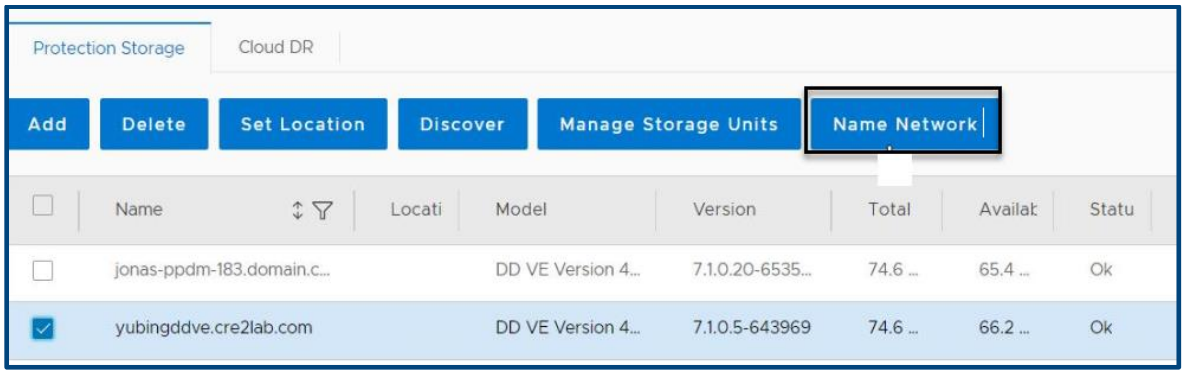
Configuration follows a multistep workflow as below as follows.



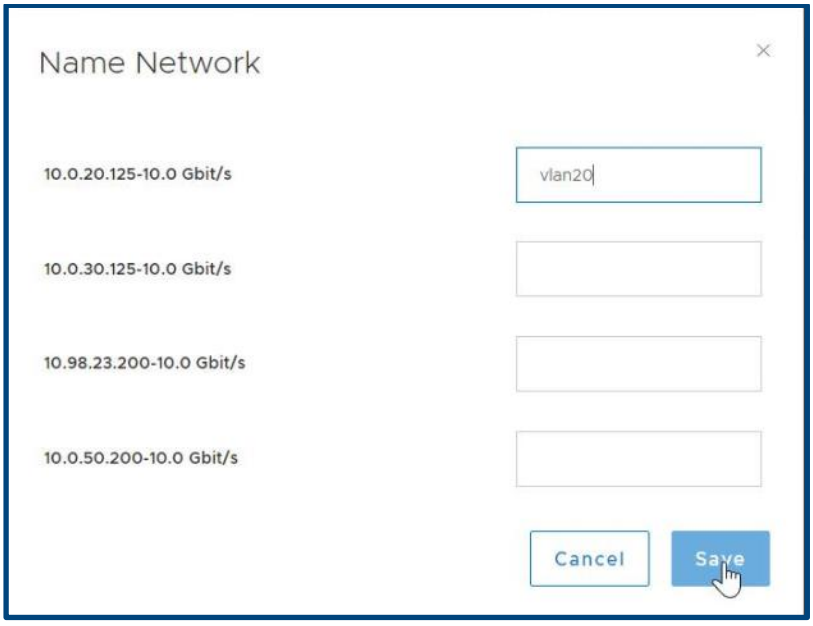
6.1.1 Discover and name PowerProtect DD series network or interface

After adding the DD series appliance as protection storage, name the virtual network between the Data Manager and the DD series appliance. To rename a virtual network (edit the network name), repeat these steps.

- Infrastructure -> Storage -> Protection Storage -> Name Network



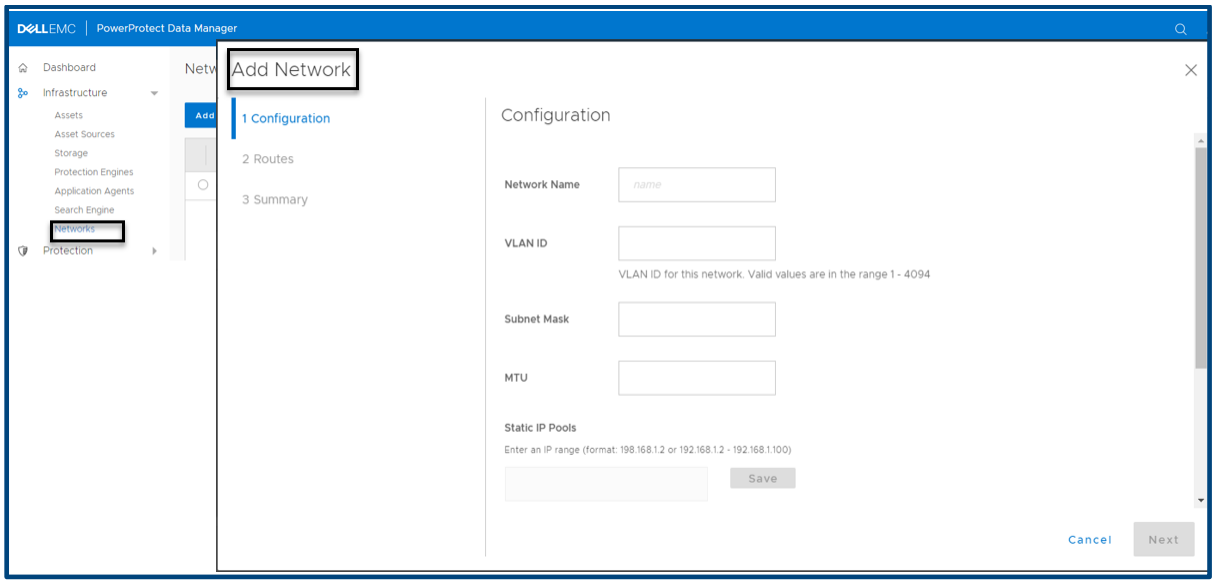
- Select the Network and add the VLAN name.



6.1.2 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 Data Manager network interface. Review the number of IP addresses needed field before you supply the required static IP addresses.

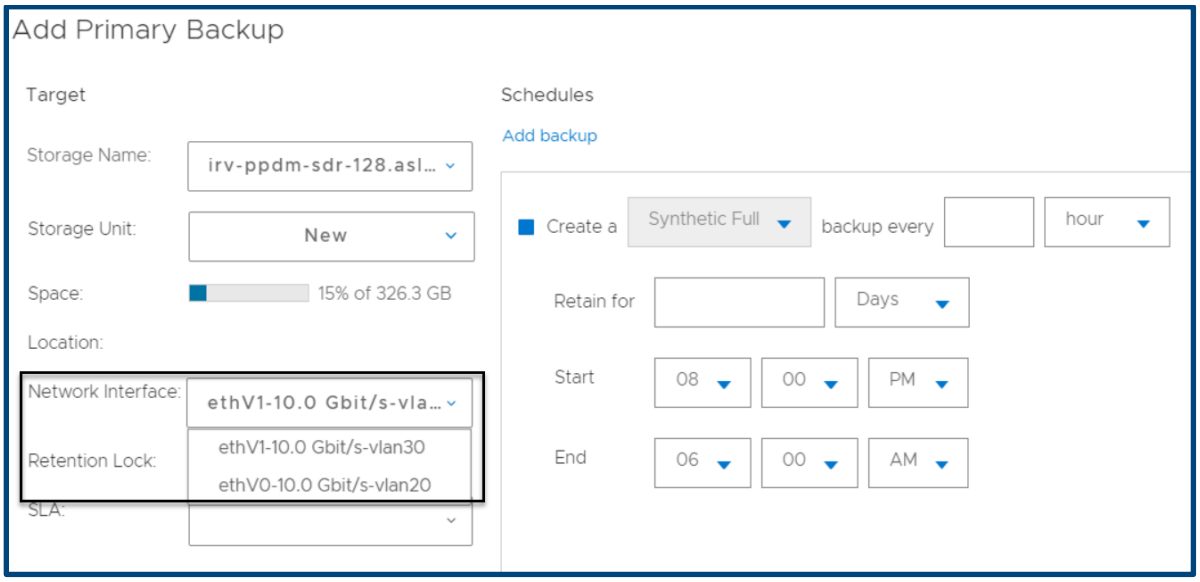
- Infrastructure -> Networks -> Add Network



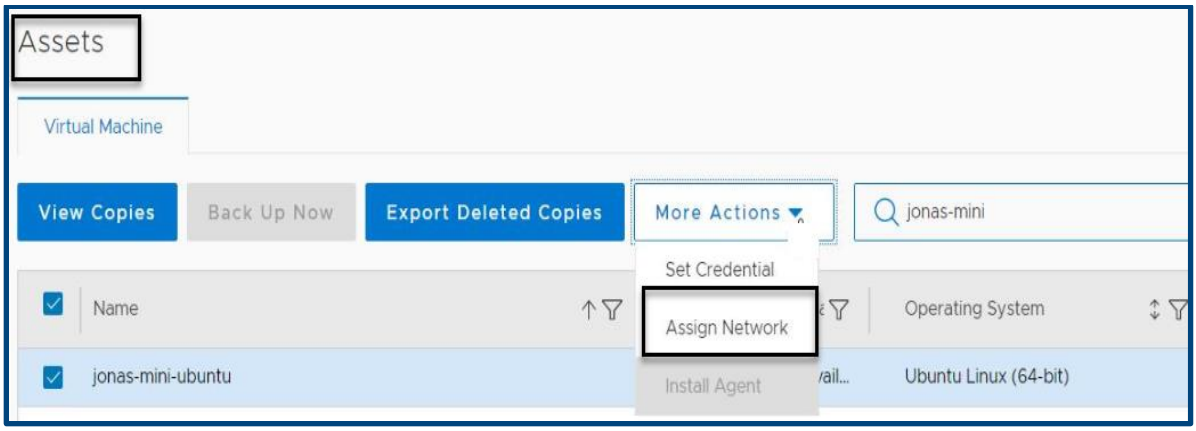
6.1.3 Assign the preferred virtual network to a Protection Policy or Asset

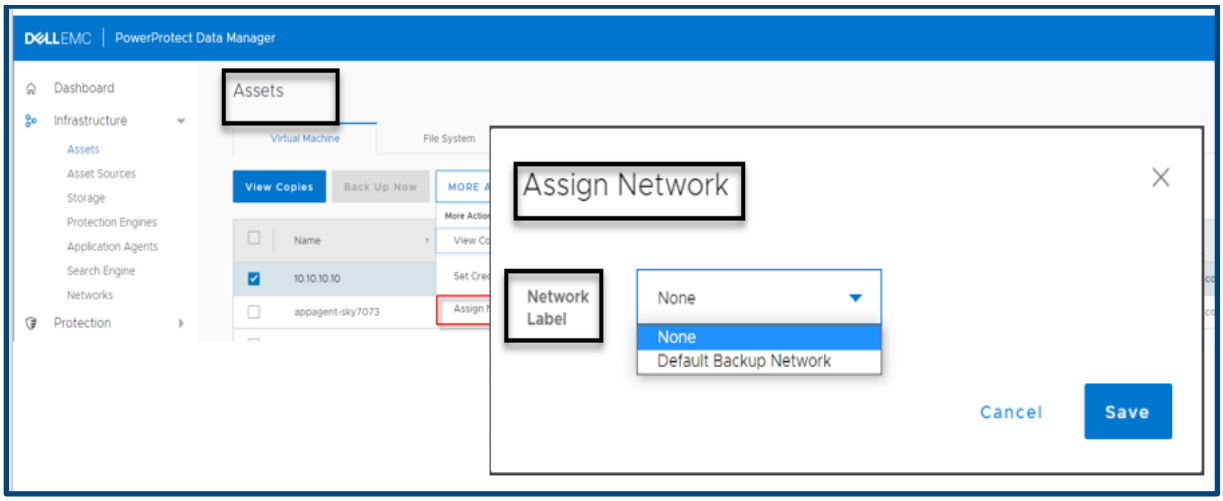
Assignments identify which assets should use each virtual network. There are two methods to associate an asset with a virtual network:

- **Using protection policy** - 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 preferred network for Primary backup and Replicate.



- **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 which are not individually assigned a virtual network will automatically use the preferred virtual network.





6.1.4 Supported Scenarios

Data Manager 19.8 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

6.2 Notes and Limitations of Multiple VLAN

Following are few considerations to keep in mind when using multiple VLANs:

- Data Manager only supports VGT mode (multi vlan) unlike vProxy which supports both VST (Single vlan) and VGT modes, hence there is no dropdown to select the Port Group for Data Manager.
- No restriction on the operation flow sequence and any parameter can be edited to modify or add values for the defined parameters.
- DD series appliance network name can be different, but Data Manager and Assets should reach the DD series appliance network. Proper naming convention helps a lot.
- Customers are responsible to ensure that network are reachable and configure them correctly.
- Old vProxy cannot be edited and attached to a VST/VGT port group, it must be reconfigured.
- It is recommended to have Data Manager and DD series appliance in same VLAN, else proper gateway/routing must be established.
- Search can only be done in the default VLAN.
- Application Data Manager asset restriction (Application and File System) – If Assets of the same host/client are attached to different networks, then those assets must be on different policy.

7 Scalability Limits for PowerProtect Data Manager

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

Component (per PowerProtect Data Manager)	Tested Limits
Number of vCenter Server supported	12 *
Number of external VM direct engines supported	40 *
Number of DD series appliances supported	10
Number of virtual machines	10,000
Maximum search engine node	5

Note:

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

Conclusion

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

A.1 Technical Support and Resources

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

Storage and data protection technical white papers and videos provide expertise that helps to ensure customer success with Dell EMC storage and data protection products.

The most up-to-date software compatibility information for PowerProtect Data Manager is provided in the E-Lab Navigator, available at https://elabnavigator.emc.com/eln/modernHomeDataProtection

A.1.1 Related Resources

PowerProtect Data Manager Administration and User Guide

PowerProtect Data Manager Deployment Guide

PowerProtect Data Manager Security Configuration Guide

DD Operation System Administration Guide