

Dell EMC PowerProtect Data Manager: Deployment and Configuration on Microsoft Azure

A next generation software platform for proven and modern cloud data protection

Abstract

This white paper describes how to deploy and configure Dell EMC PowerProtect Data Manager on Microsoft Azure for seamless protection of workloads on Azure cloud.

October 2021

Revisions

Date	Description
June 2021	Initial release
October 2021	White paper updated with PowerProtect Data Manager v19.9 release updates

Acknowledgments

Author: Vinod Kumar Kumaresan

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

This document may contain certain words that are not consistent with Dell's current language guidelines. Dell plans to update the document over subsequent future releases to revise these words accordingly.

This document may contain language from third party content that is not under Dell's control and is not consistent with Dell's current guidelines for Dell's own content. When such third-party content is updated by the relevant third parties, this document will be revised accordingly.

Copyright © 2021 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. [10/21/2021] [Technical White Paper] [H18800.1]

Table of contents

Revisions.....	2
Acknowledgments.....	2
Table of contents	3
Executive summary.....	4
Audience	4
1 Introduction.....	5
1.1 Dell EMC PowerProtect Data Manager for Azure	5
1.2 Basic architecture Overview	6
1.3 Azure data transfer costs.....	6
2 Deploying Data Manager and DDVE on Azure	7
2.1 Deploying Data Manager and DDVE on Azure	8
3 Manual Configuration of Data Manager deployed on Azure	18
A Technical support and resources	24
A.1 Related resources.....	24

Executive summary

As more enterprises adopt a multi-cloud strategy, leveraging a common data protection solution across the on-premises infrastructure and the public cloud will enable enterprises to achieve operational efficiencies and lower costs.

For organizations that have workloads running in Azure cloud and need self-service backup and restores from enterprise application tools, Dell EMC PowerProtect Data Manager provides data protection of workloads in Microsoft Azure and Azure Government.

Data owners and administrators can deploy Data Manager with automation from the Azure Marketplace to protect business-critical workloads in the cloud. Data Manager enables the protection of traditional workloads including Oracle, SQL, SAP HANA, and file systems and cloud native applications running in Kubernetes containers. Easy to install and deploy from the Azure Marketplace, Data Manager and Dell EMC PowerProtect DD Virtual Edition (DDVE) provide high levels of performance and deduplication.

Audience

This white paper is intended for Dell Technologies customers, partners, and employees looking for options to protect the workloads hosted on Azure cloud using Data Manager and DDVE.

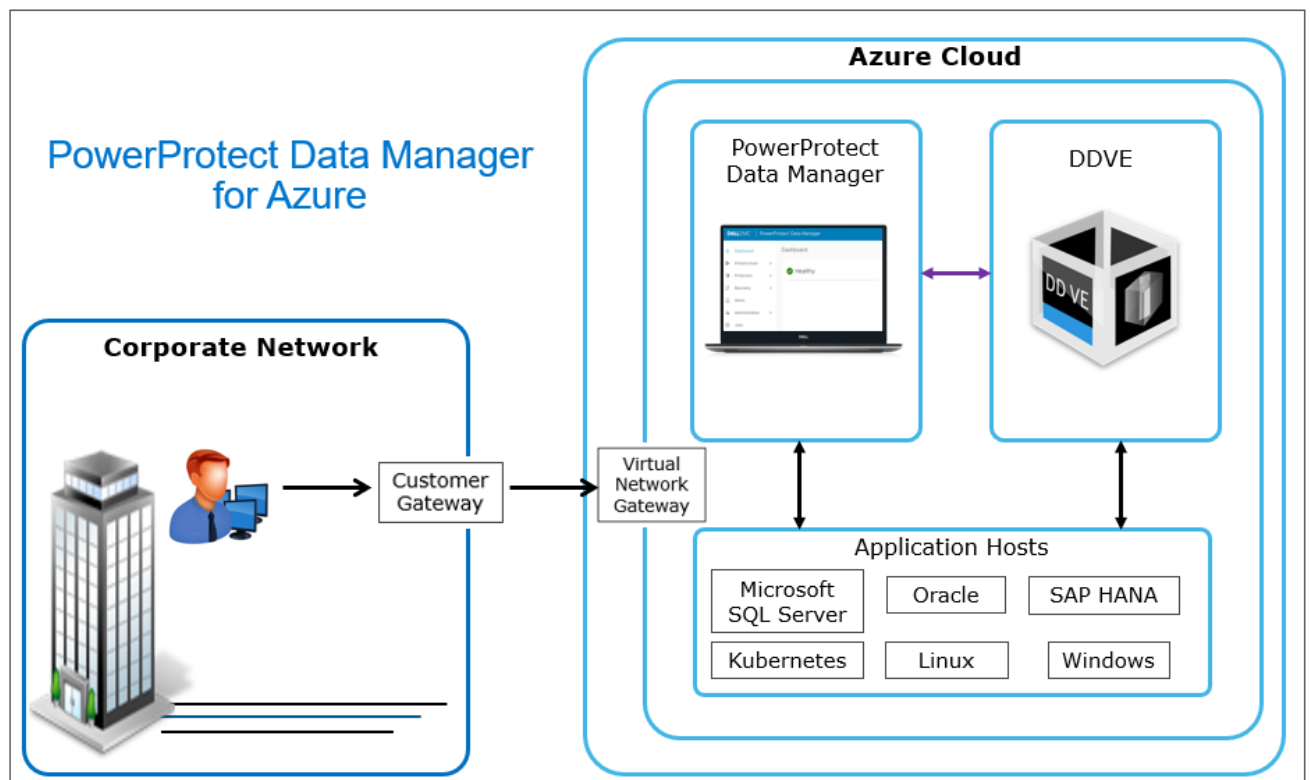
1 Introduction

1.1 Dell EMC PowerProtect Data Manager for Azure

Data Manager software is an enterprise solution that provides software-defined data protection, deduplication, operational agility, self-service, and IT governance. Data Manager for Azure provides protection for cloud-based assets such as the following:

- Oracle, SQL, and SAP HANA databases
- Virtual machines in Azure VMware Solution for Azure
- Kubernetes clusters deployed to Azure
- File systems

Data Manager and DDVE can be deployed as one package from the Azure Marketplace. DDVE on Azure can also be deployed outside of the Data Manager deployment process. DDVE scales up to 256TB per instance in-cloud and supports Azure Government. Data Manager includes a 90-day trial license by default.

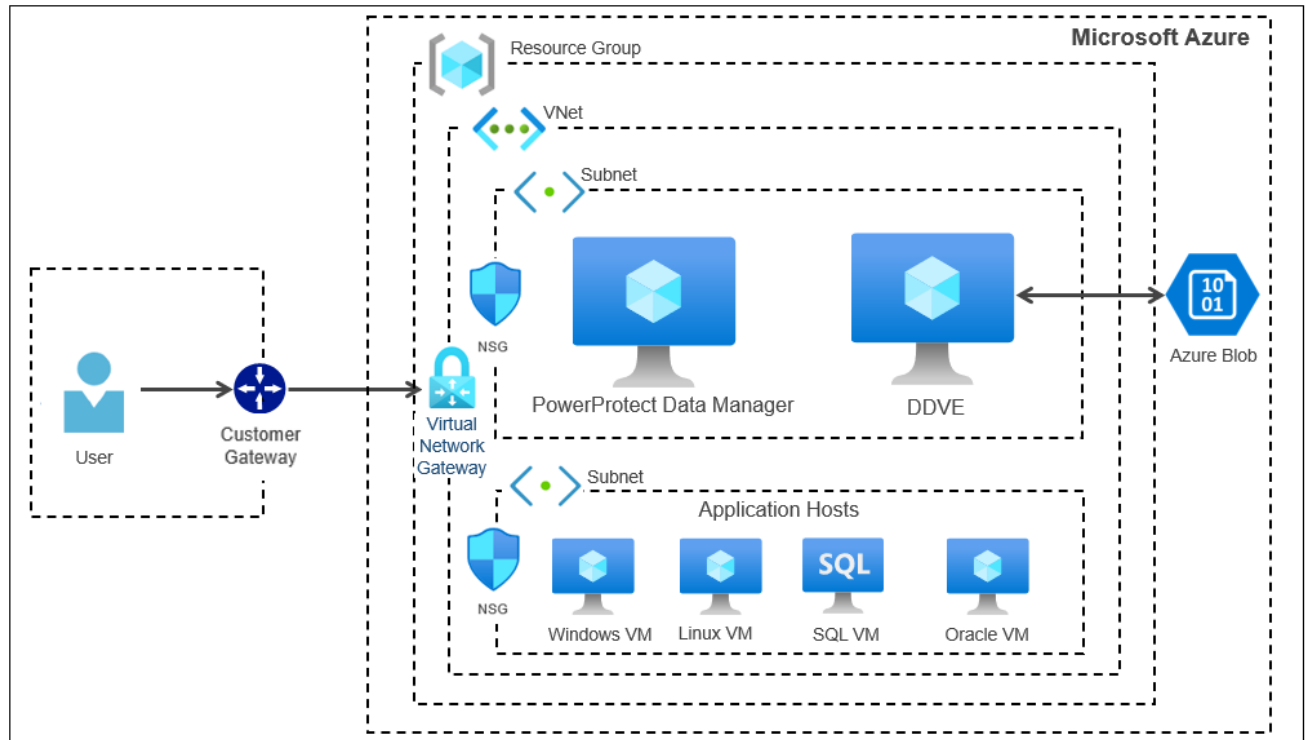


Using Microsoft Azure Resource Manager (ARM), Data Manager can be deployed to a virtual appliance in an Azure cloud. Data Manager is deployed with a private IP address. A VPN connection configuration is required to access Data Manager from an external site.

Data Manager deployed on Azure cloud requires DDVE as the protection storage appliance. DDVE is a software-only protection storage appliance that provides data protection for entry, enterprise, and service-provider environments. With Data Manager and DDVE on Azure, the business-critical workloads deployed on Azure cloud can be protected.

1.2 Basic architecture Overview

The following diagram represents the basic architecture of Data Manager on Azure. The diagram shows a possible distribution of Data Manager and DDVE in one private subnet, and application hosts in another.



Access to Data Manager and DDVE is managed by Virtual Network (VNet) service endpoints and their policies, and by network and application security groups. DDVE uses blob containers to store the backed-up data of virtual appliances and virtual machines deployed to Azure. Sensitive Data Manager data, such as passwords, is encrypted and stored in a lockbox.

1.3 Azure data transfer costs

Microsoft charges a monthly fee based on the amount and types of data transferred by Data Manager and DDVE in an Azure cloud.

Consider the following information when planning the Azure architecture:

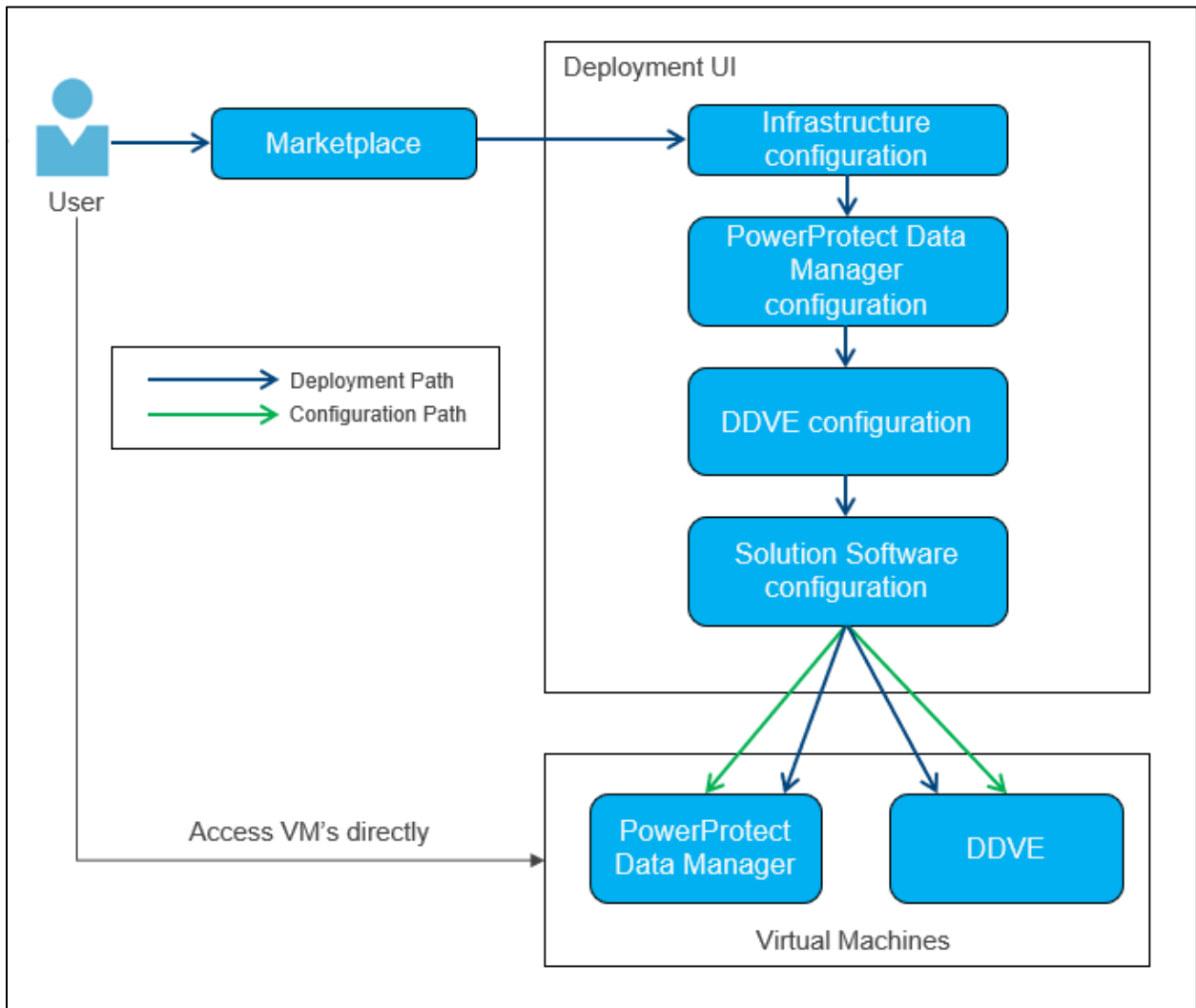
- In an Azure cloud, most of the data transferred is between the hosts being protected and DDVE
- If Kubernetes is being used, data is also transferred between the protection engine hosts and DDVE
- Microsoft does not have data transfer fees for hosts that are in the same region

For current details of all Microsoft data transfer costs and other fees, see [Bandwidth Pricing Details](#) and the [Pricing Calculator](#).

Note: To minimize data transfer costs, and to minimize the path that data transfers take, use as few availability zones and regions as possible.

2 Deploying Data Manager and DDVE on Azure

The following shows the high-level deployment steps for Data Manager and DDVE on Azure.

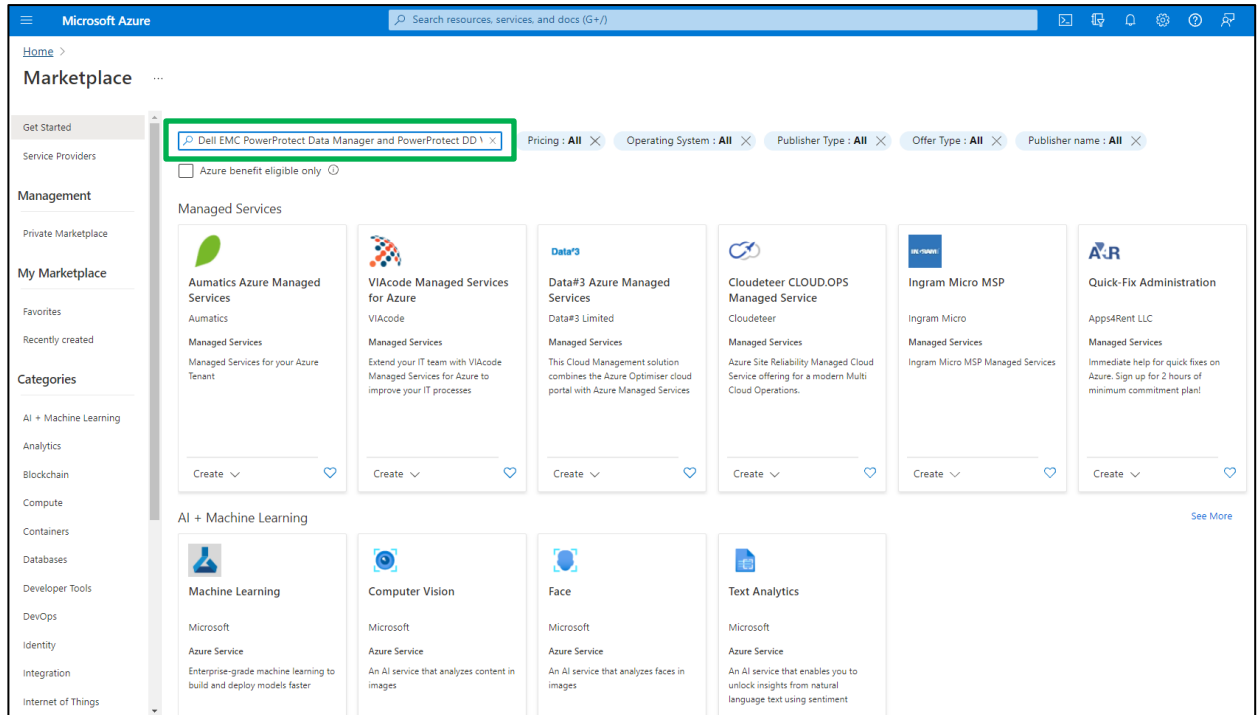


Starting with Data Manager version 19.9, DDVE can be configured at the same time as Data Manager when they are deployed to Microsoft Azure using solution software configuration option.

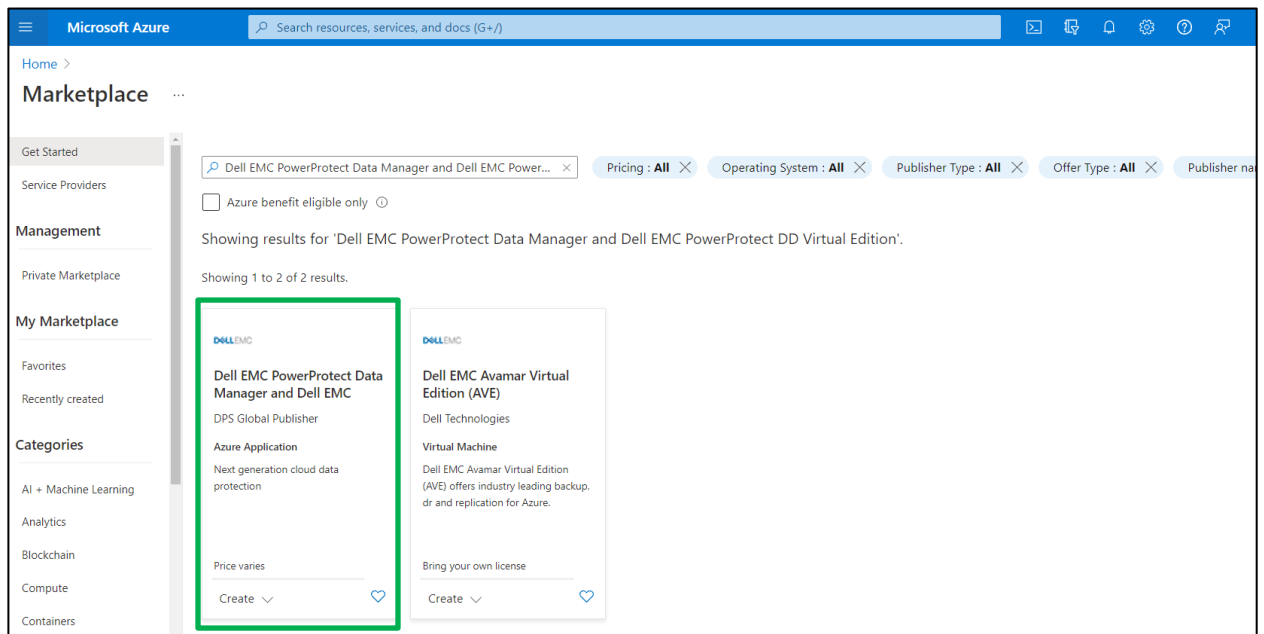
For successful deployment of Data Manager and DDVE on Azure, see [Dell EMC PowerProtect Data Manager Azure Deployment Guide](#) and [Dell EMC PowerProtect DDVE on Azure Installation and Administration Guide](#) for more details on preparing for deployment, deployment requirements, and networking interoperability.

2.1 Deploying Data Manager and DDVE on Azure

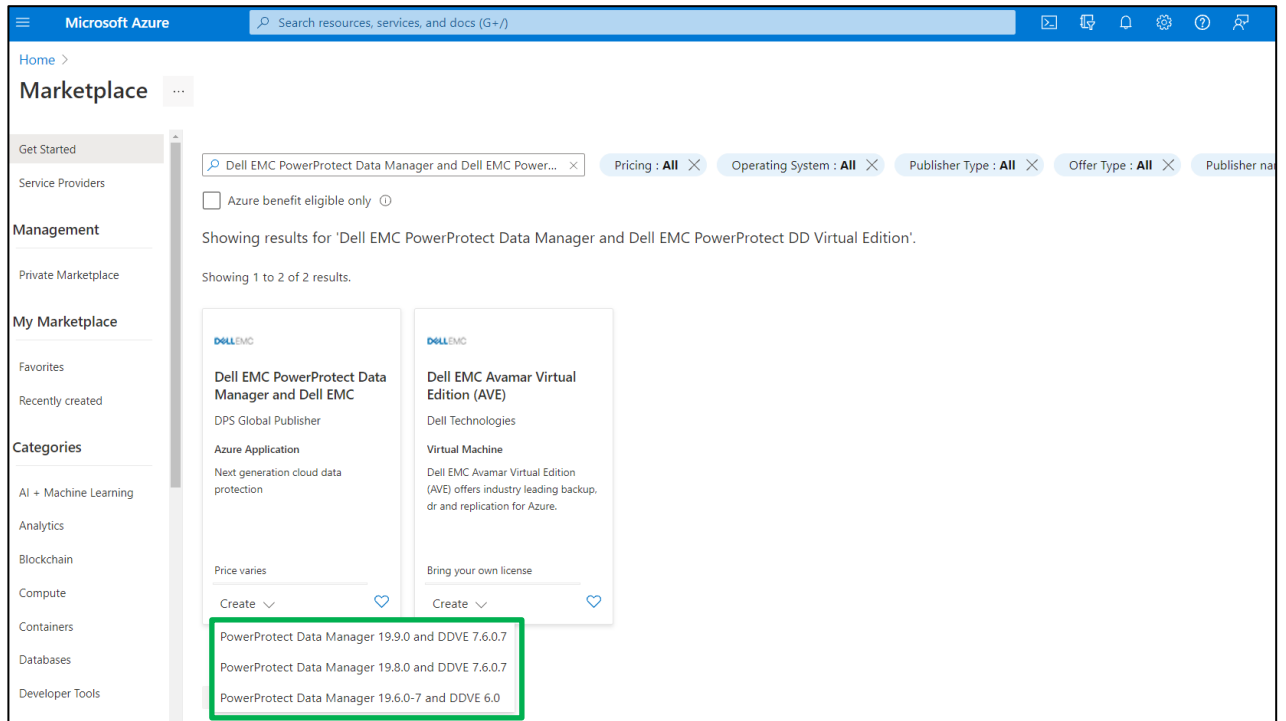
1. In a browser, navigate to <https://portal.azure.com>
2. Log in to the Azure account.
3. From the **Home > Marketplace > Get Started** pane, select Search the Marketplace and search for **“Dell EMC PowerProtect Data Manager and PowerProtect DD Virtual Edition”**.



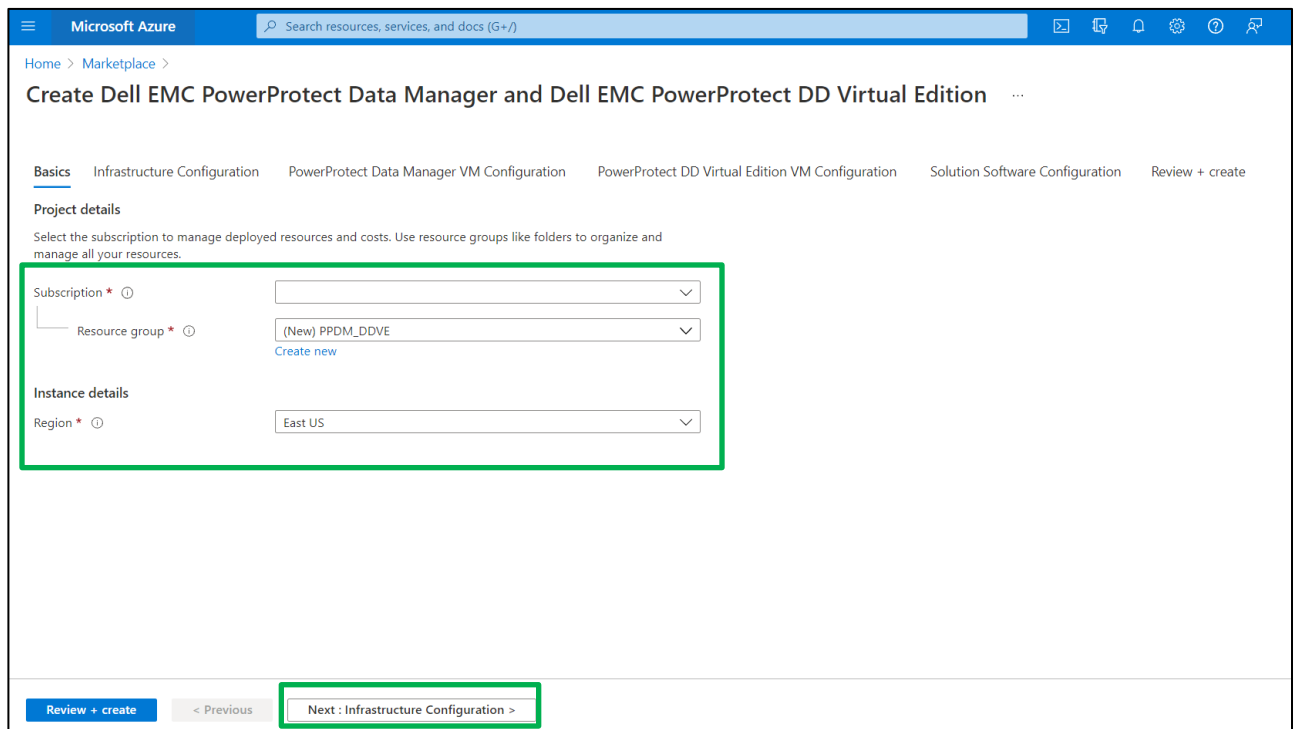
4. Choose **Dell EMC PowerProtect Data Manager and PowerProtect DD Virtual Edition** and select **Create**.



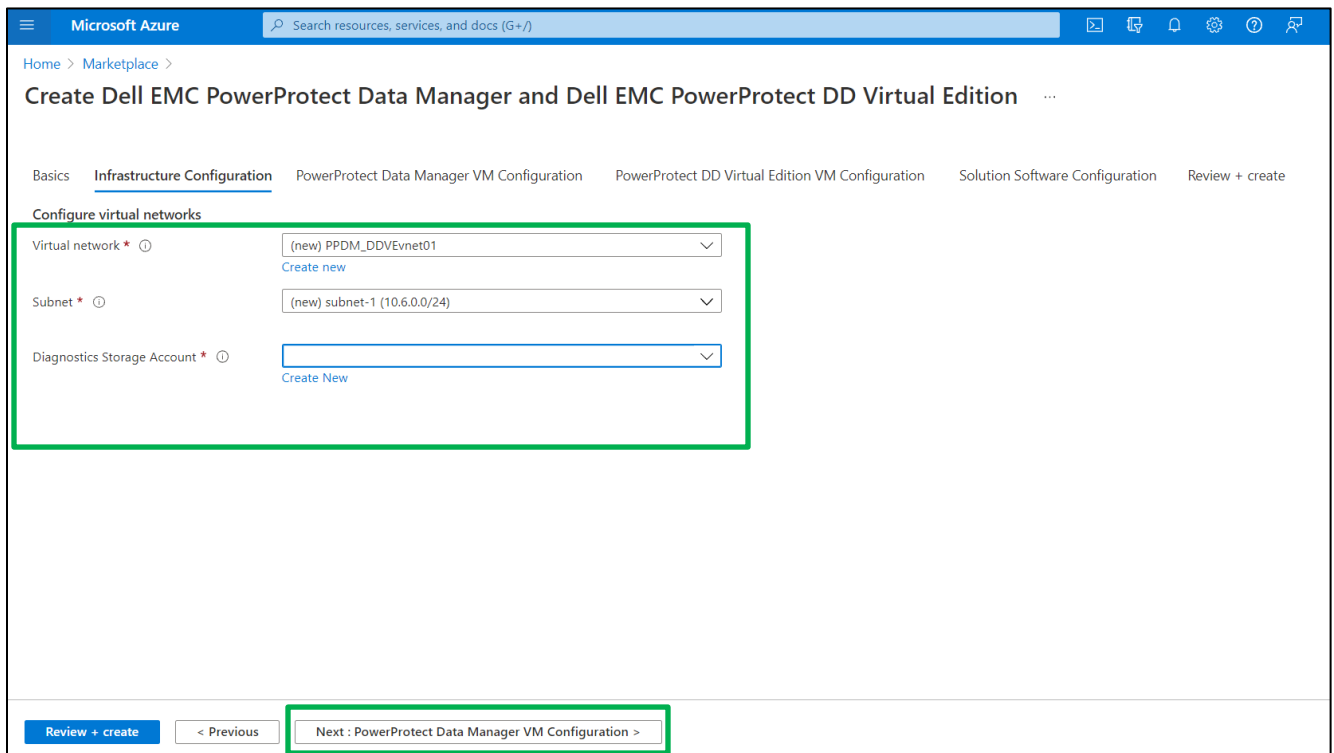
- Select the required Data Manager and DDVE version from the list. For example, **“PowerProtect Data Manager 19.9.0 and DDVE 7.6.07”**.



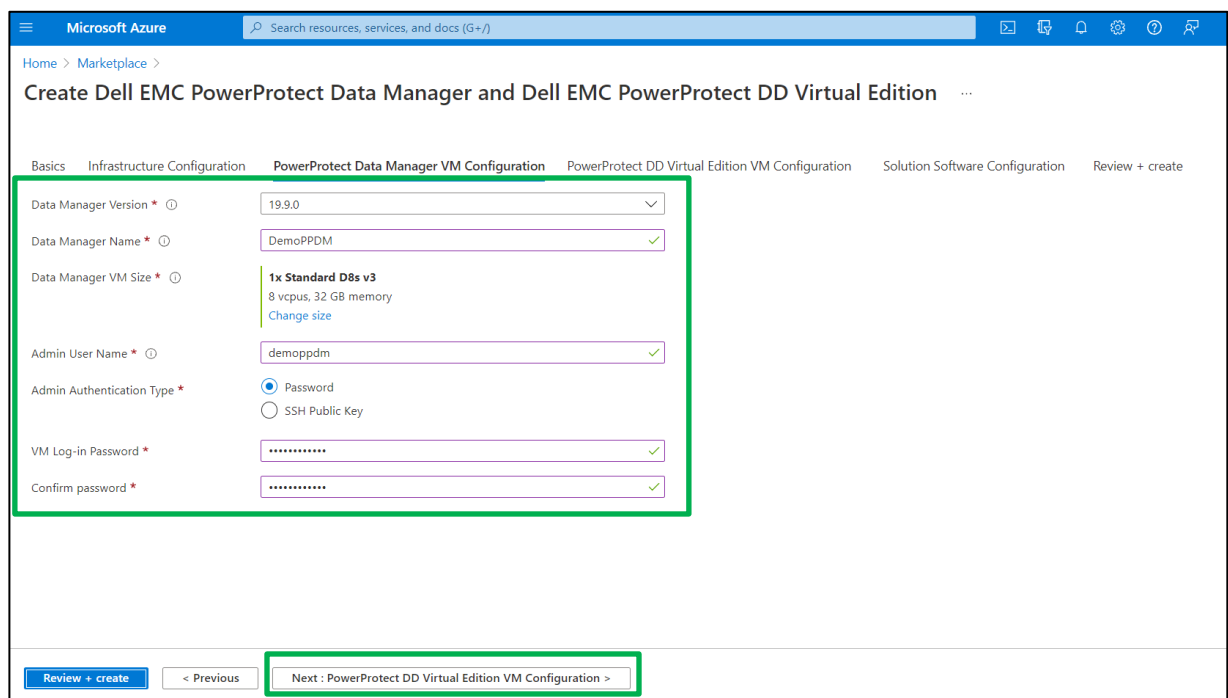
- From the **Home > Marketplace > Create Dell EMC PowerProtect Data Manager and PowerProtect DD Virtual Edition > Basics** pane, provide the project and instance details. Click **Next: Infrastructure Configuration**.



- From the **Home > Create Dell EMC PowerProtect Data Manager and PowerProtect DD Virtual Edition > Infrastructure Configuration** pane, configure the virtual networks and storage account. Click **Next: PowerProtect Data Manager VM Configuration**.

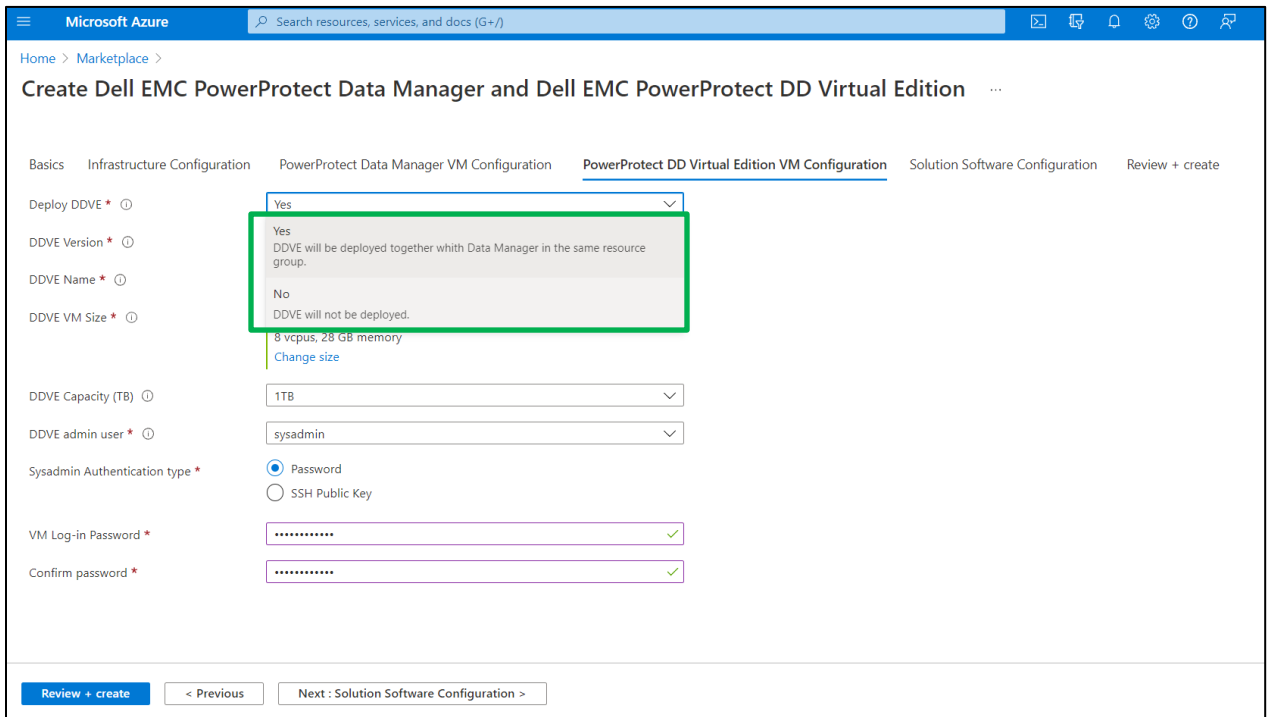


- From the **Home > Create Dell EMC PowerProtect Data Manager and PowerProtect DD Virtual Edition > PowerProtect Data Manager VM Configuration** pane, configure Data Manager and click **Next: PowerProtect DD Virtual Edition VM Configuration**.

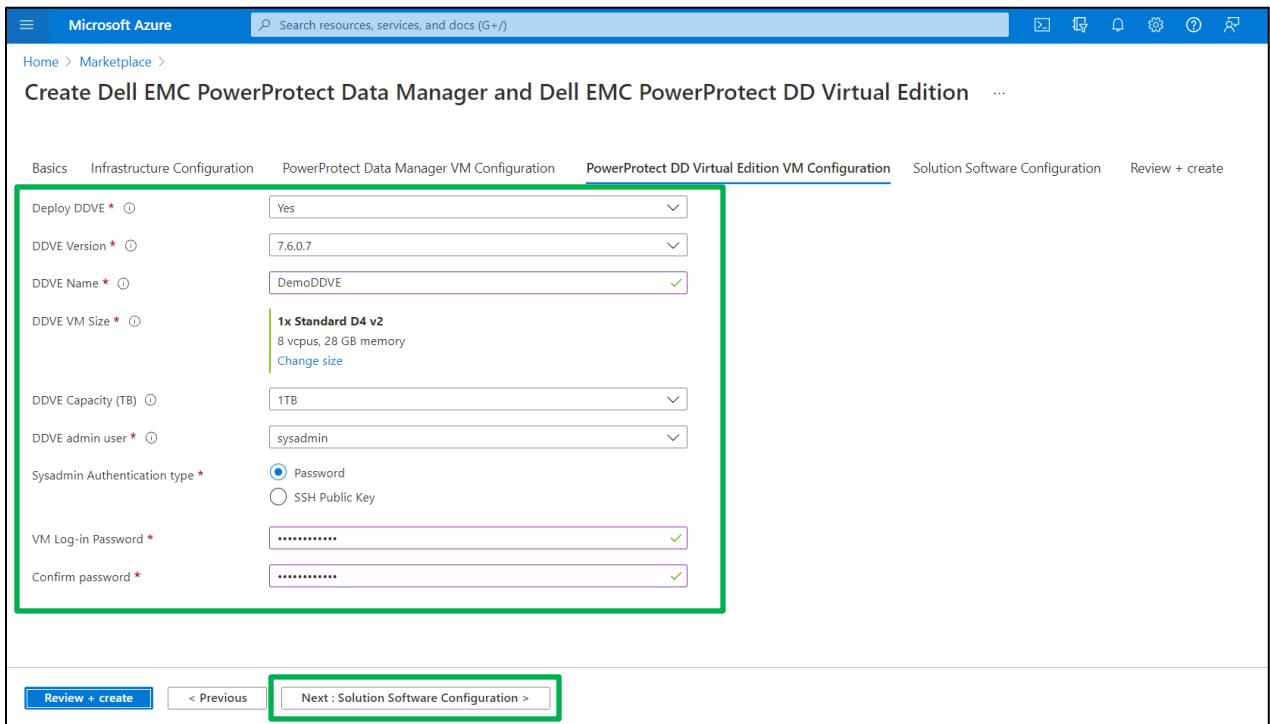


9. From the **PowerProtect DD Virtual Edition VM Configuration** pane,

- Select **Yes** to deploy and launch a DDVE instance in the same subnet as Data Manager.
- Select **No** to deploy only Data Manager.



If you selected **Yes**, configure the DDVE instance and click **Next: Solution Software Configuration**.



Note: You might choose not to deploy DDVE if you already have an instance deployed, or if you are performing PowerProtect Data Manager-server disaster recovery.

10. From the **Home > Create Dell EMC PowerProtect Data Manager and Data Domain Virtual Editions > Solution Software Configuration** pane,

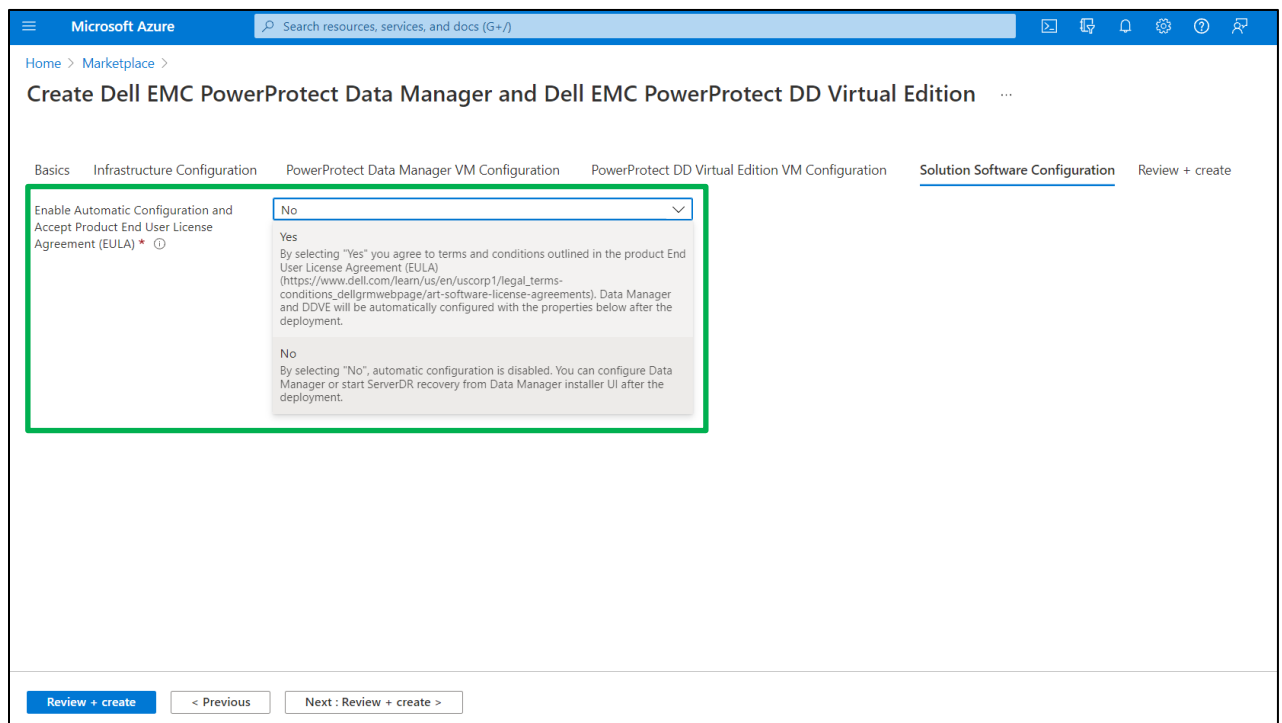
- Select **Yes** to accept the EULA.

Note: By selecting **Yes**, you agree to accept the terms and conditions outlined in the product End User License Agreement (EULA). Do not select **Yes** if you need to restore a Data Manager disaster-recovery backup.

- Select **No** if you do not accept the EULA.

Note: If you select **No**, automatic configuration is disabled. Data Manager and DDVE must be manually configured after they are deployed.

The following shows the option to **Enable Automatic Configuration and Accept Product End User License Agreement (EULA)**.



Note: Solution software configuration option is available starting with Data Manager version 19.9.

11. If you selected **Yes**, Data Manager and DDVE will be automatically configured after the deployment, with the properties shown below. Click **Next: Review + create**.

Microsoft Azure

Home > Marketplace >

Create Dell EMC PowerProtect Data Manager and Dell EMC PowerProtect DD Virtual Edition

Basics Infrastructure Configuration PowerProtect Data Manager VM Configuration PowerProtect DD Virtual Edition VM Configuration **Solution Software Configuration** Review + create

Enable Automatic Configuration and Accept Product End User License Agreement (EULA) * Yes

Data Manager Software Configuration

Data Manager Time Zone * UTC - Coordinated Universal Time

Data Manager NTP Servers

Data Manager common password * ✓

Confirm password * ✓

DDVE Software Configuration

Storage Account Name * demotme ✓

Container Name * demotme ✓

Storage Access Key * s3Slsc10Nqs433KkhsnWTQivTmMk9gSDbo0tdA74AIPjYBEscqO6QcQ... ✓

DDVE common password * ✓

Confirm password * ✓

[Review + create](#) < Previous **Next: Review + create >**

12. From the **Home > Create Dell EMC PowerProtect Data Manager and PowerProtect DD Virtual Editions > Review + create** pane, click **Create**.

Microsoft Azure

Home > Marketplace >

Create Dell EMC PowerProtect Data Manager and Dell EMC PowerProtect DD Virtual Edition ...

Validation Passed

Basics Infrastructure Configuration PowerProtect Data Manager VM Configuration PowerProtect DD Virtual Edition VM Configuration Solution Software Configuration **Review + create**

PRODUCT DETAILS

Dell EMC PowerProtect Data Manager and Dell EMC PowerProtect DD Virtual Edition
by DPS Global Publisher
[Terms of use](#) | [Privacy policy](#)

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Basics

Subscription	
Resource group	PPDM_DDVE
Region	East US

Infrastructure Configuration

Virtual network	PPDM_DDVEvnet01
Subnet	subnet-1
Address prefix (Subnet)	10.6.0.0/24
Diagnostics Storage Account	

PowerProtect Data Manager VM Configuration

Data Manager Version	19.9.0
Data Manager Name	DemoPPDM
Data Manager VM Size	Standard_D8s_v3
Admin User Name	demoppdm
VM Log-in Password	*****

PowerProtect DD Virtual Edition VM Configuration

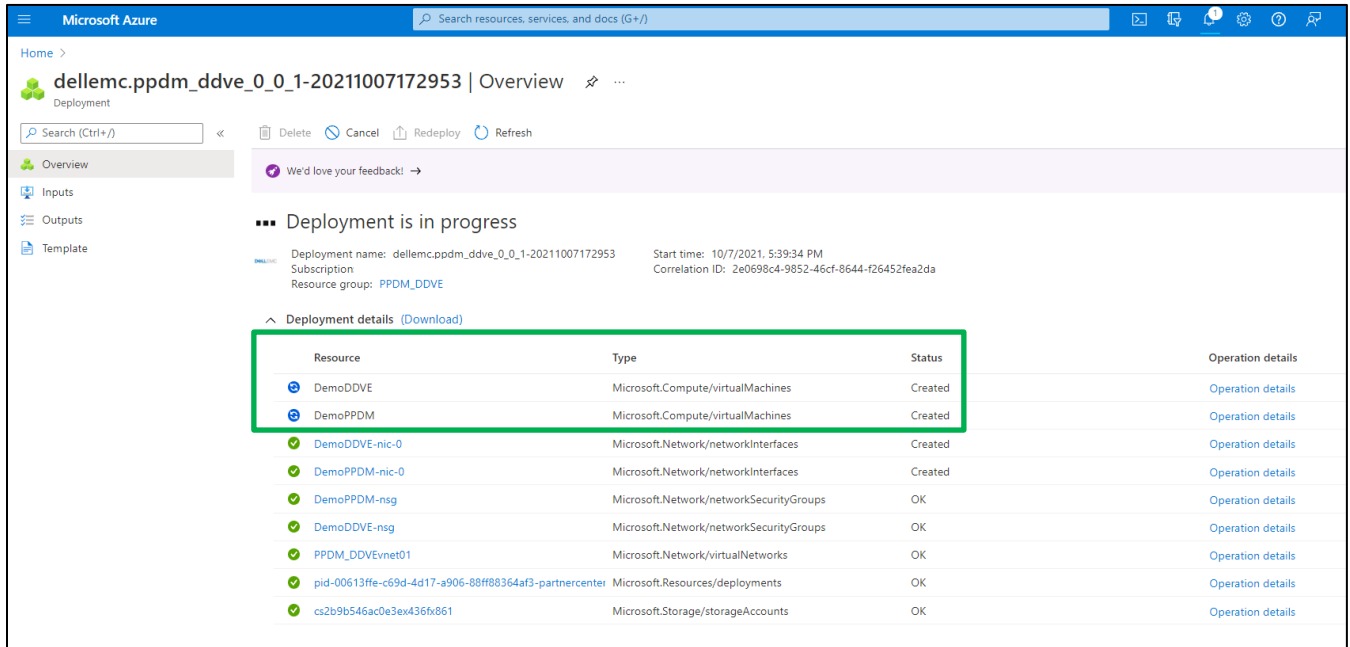
Deploy DDVE	Yes
DDVE Version	7.6.0.7
DDVE Name	DemoDDVE
DDVE VM Size	Standard_D4_v2
DDVE Capacity (TB)	1TB
DDVE admin user	sysadmin
VM Log-in Password	*****

Solution Software Configuration

Enable Automatic Configuration and AC...	Yes
Data Manager Time Zone	UTC - Coordinated Universal Time
Data Manager NTP Servers	-
Data Manager common password	*****
Storage Account Name	demotme
Container Name	demotme
Storage Access Key	zuUCd/Pqjr+zEvvwK63zCGV215Jps8xNBgjBO+tlJpp/SL3c8ILGxYOoCVNSB6r...
DDVE common password	*****

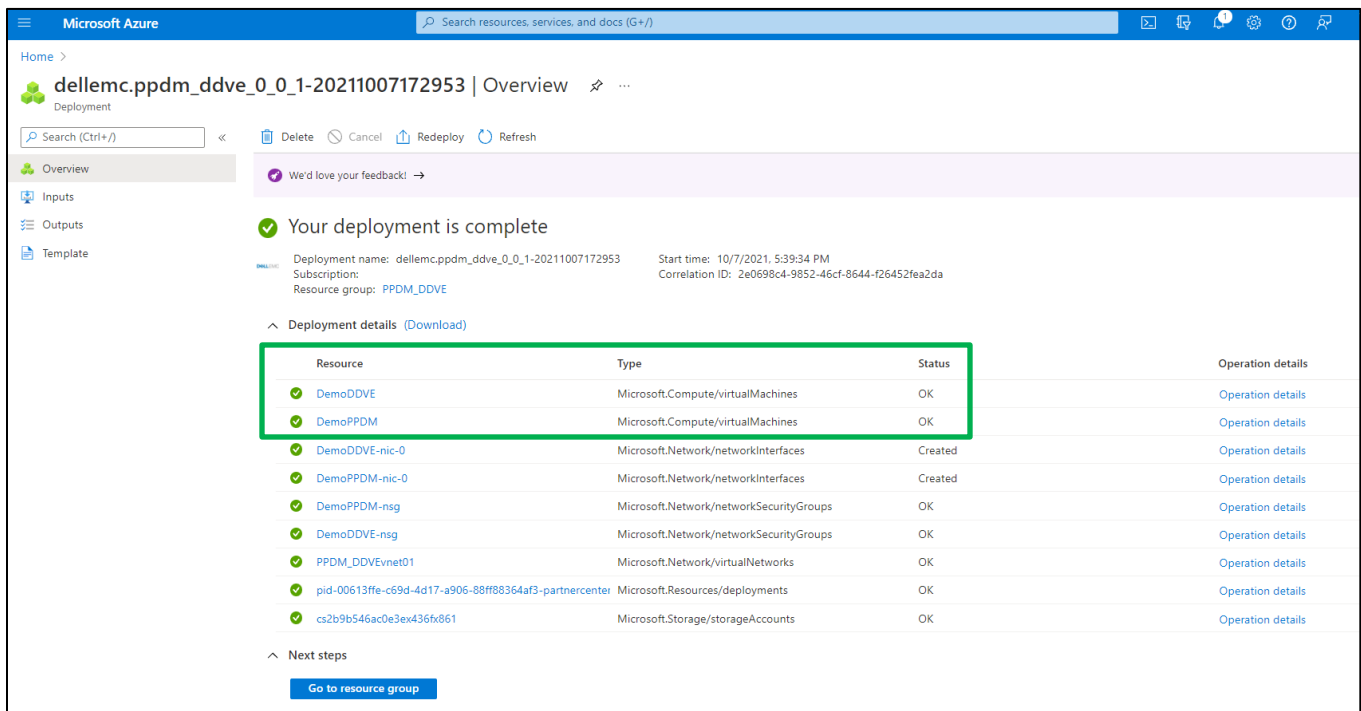
Create < Previous Next Download a template for automation

The following figure shows the Data Manager and DDVE deployments in progress.



Note: This takes between approximately 20 and 25 minutes, depending on whether automatic configuration is enabled.

13. When the Data Manager and DDVE deployment are complete, select **Go to resource group** to view the Data Manager instance details.



The following figures show that the Data Manager and DDVE instances are running.

Data Manager instance

The screenshot displays the Azure portal interface for a virtual machine named 'DemoPPDM'. The 'Essentials' section shows the VM is running in the 'PPDM_DDVE' resource group, located in the 'East US' region. The 'Properties' section provides detailed specifications for the virtual machine.

Category	Property	Value
Essentials	Resource group (change)	PPDM_DDVE
	Status	Running
	Location	East US
	Subscription (change)	-
	Subscription ID	-
	Tags (change)	Click here to add tags
	Operating system	Linux (suse 12)
	Size	Standard D8s v3 (8 vcpus, 32 GiB memory)
	Public IP address	-
	Virtual network/subnet	PPDM_DDVEvnet01/subnet-1
DNS name	-	
Properties	Computer name	demoppdm
	Operating system	Linux (suse 12)
	Publisher	dellemc
	Offer	ppdm_0_0_1
	Plan	powerprotect-data-manager-19-9-0-13
	VM generation	V1
	Agent status	Ready
	Agent version	2.4.0.2
	Host group	None
	Host	-
	Proximity placement group	-
	Colocation status	N/A
	Capacity reservation group	-
	Public IP address	-
	Private IP address (IPv6)	-
Private IP address	10.6.0.4	
Private IP address (IPv6)	-	
Virtual network/subnet	PPDM_DDVEvnet01/subnet-1	
DNS name	-	
Size	Size	Standard D8s v3
	vCPUs	8
	RAM	32 GiB
Disk	OS disk	DemoPPDM-osdisk
	Azure disk encryption	Not enabled

DDVE instance

The screenshot displays the Azure portal interface for a virtual machine named 'DemoDDVE'. The 'Essentials' section shows the VM is running in the 'PPDM_DDVE' resource group, located in the 'East US' region. The 'Properties' section provides detailed specifications for the virtual machine.

Category	Property	Value
Essentials	Resource group (change)	PPDM_DDVE
	Status	Running
	Location	East US
	Subscription (change)	-
	Subscription ID	-
	Tags (change)	Click here to add tags
	Operating system	Linux
	Size	Standard D4 v2 (8 vcpus, 28 GiB memory)
	Public IP address	-
	Virtual network/subnet	PPDM_DDVEvnet01/subnet-1
DNS name	-	
Properties	Computer name	DemoDDVE
	Operating system	Linux
	Publisher	dellemc
	Offer	dell-erc-datadomain-virtual-edition-v4
	Plan	ddve-7607
	VM generation	V1
	Agent status	Not Ready
	Agent version	Unknown
	Host group	None
	Host	-
	Proximity placement group	-
	Colocation status	N/A
	Capacity reservation group	-
	Public IP address	-
	Public IP address (IPv6)	-
Private IP address	10.6.0.5	
Private IP address (IPv6)	-	
Virtual network/subnet	PPDM_DDVEvnet01/subnet-1	
DNS name	-	
Size	Size	Standard D4 v2
	vCPUs	8
	RAM	28 GiB
Disk	OS disk	DemoDDVE-osdisk
	Azure disk encryption	Not enabled

See [Dell EMC PowerProtect Data Manager Azure Deployment Guide](#) for more details on Data Manager deployment to Azure.

Note: The Data Manager and DDVE instance deployment takes a few minutes to start and initialize.

See [Dell EMC PowerProtect DDVE on Azure Installation and Administration Guide](#) for details on how to configure the DDVE instance deployed on Azure.

3 Manual Configuration of Data Manager deployed on Azure

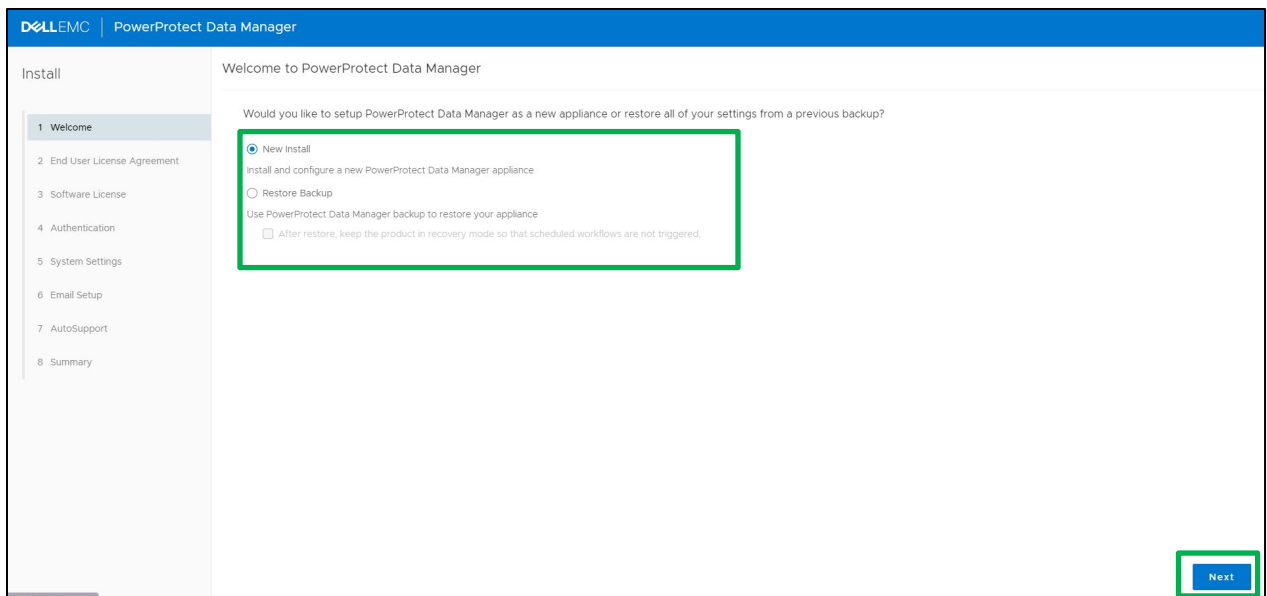
After the PowerProtect Data Manager instance is deployed, it is referred to as a virtual appliance. After the virtual appliance is started, you might need to configure it.

Perform the following steps from a host that has access to the virtual appliance.

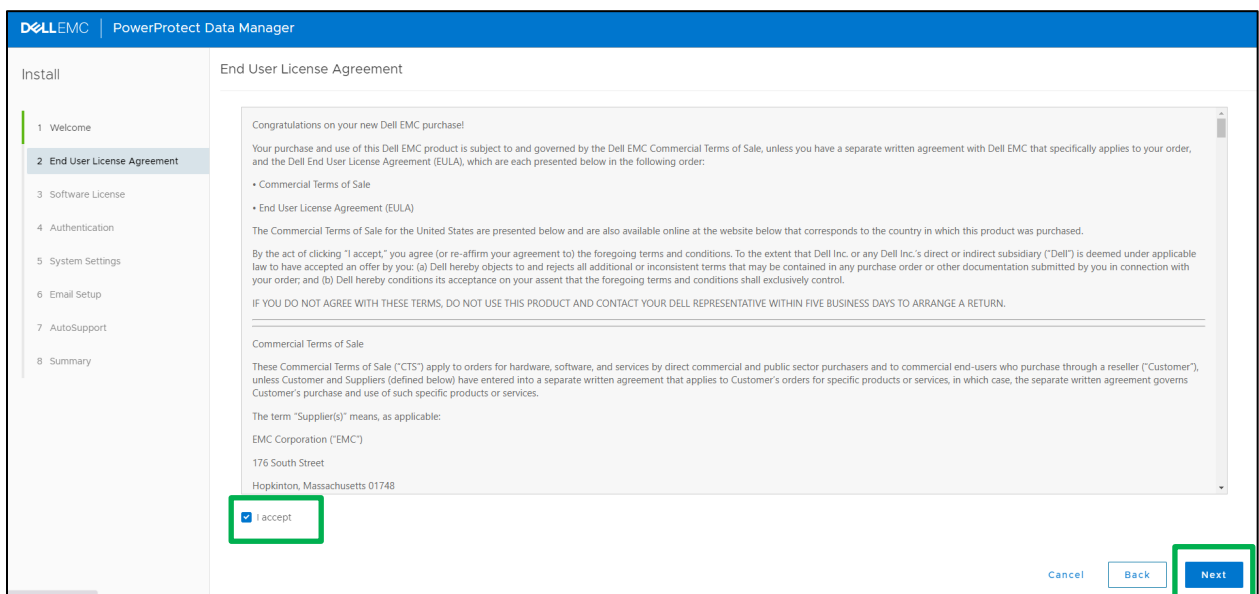
1. From a host that has network access to Data Manager, use Google Chrome connect to the appliance: **https://<appliance_hostname or IP address>**.

Note: To connect to the appliance by its hostname, you must configure DNS.

2. On the **Welcome** page, select **New Install** to set up Data Manager as a new installation and click **Next**.



3. Review the **End User License Agreement**, choose **I accept**, and select **Next**.

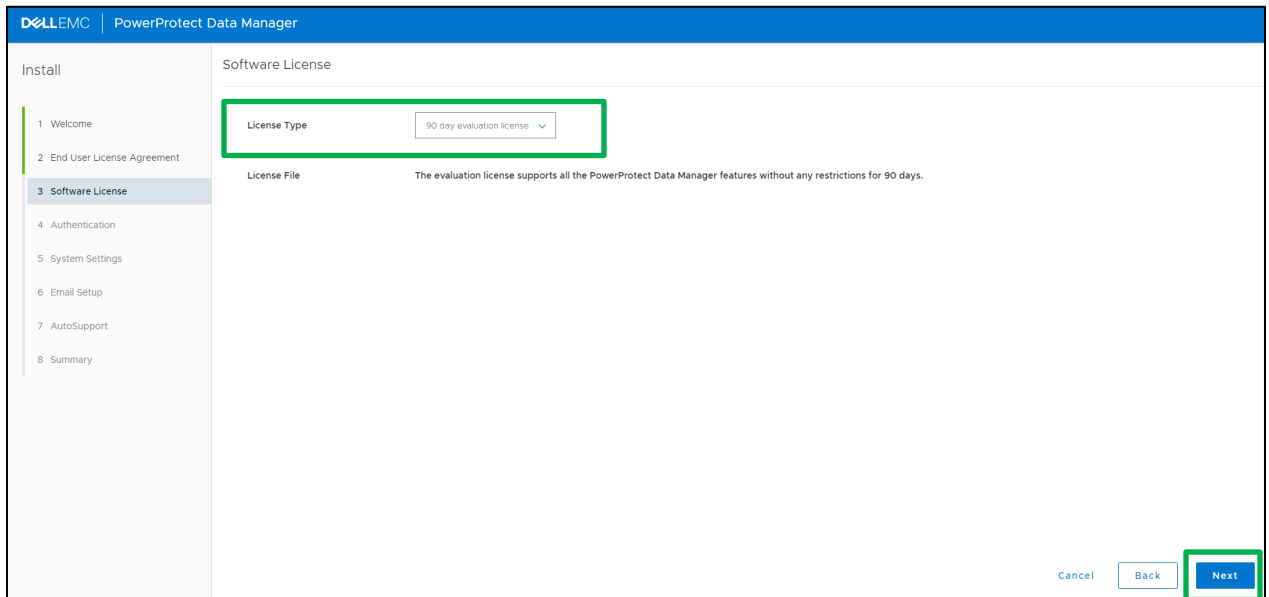


4. On the **Software License** pane, perform the following actions:

a. In the **License Type** field, select a type of license.

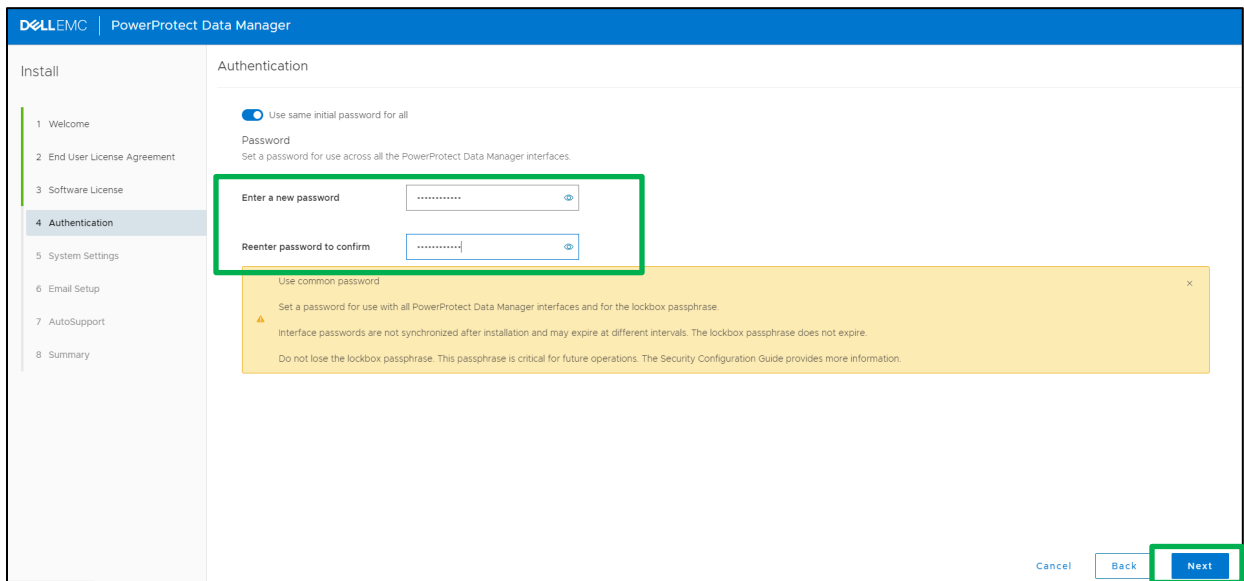
- To use an evaluation license, select **90 days evaluation license**.
- To load a license, select **License File > Choose File** and browse to and select the license file to load.
- To copy the contents of the license file, select **Plain Text** and copy the contents of the license file into the Plain Text field.

b. Click **Next**.



5. In the **Authentication** pane, perform the following actions:

The **Use common password** option is selected by default. This toggle sets one initial password for use with all Data Manager interfaces.



a. Optionally, clear the **Use common password** option.

If the **Use common password** option is selected, in the **Enter a new password** and **Reenter password to confirm** fields, specify a password.

If the **Use common password** option is not selected, in the **Enter a new password** and **Reenter password to confirm** fields, specify individual passwords for the interfaces.

Ensure that the password meets the following requirements:

- A minimum of nine characters and a maximum of one hundred characters
- At least one numeric character (0-9)
- At least one uppercase character (A-Z)
- At least one lowercase character (a-z)
- At least one special character from the following list of acceptable characters:
!@#\$%^&*()_+=~{}[]<>?/\`.;|' (Spaces are allowed)

b. Click **Next**.

6. In the **System Settings** pane, perform the following actions:

a. In the **Current Timezone** list box, select the time zone where the system is physically located.

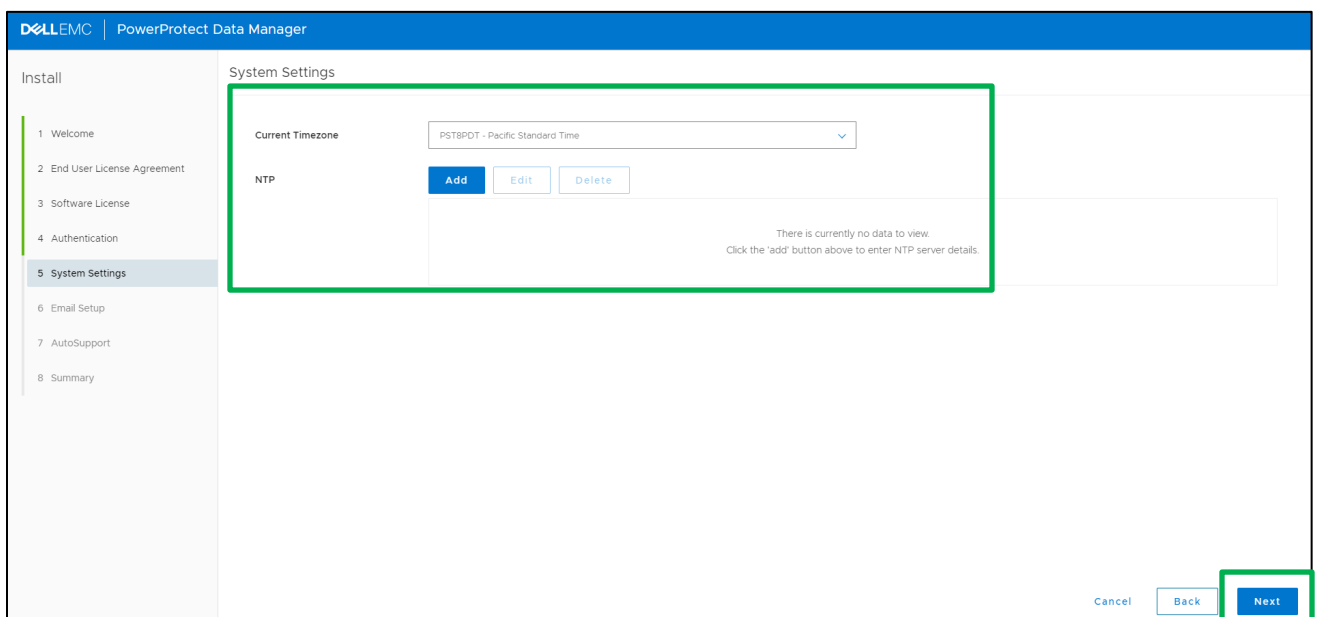
b. To add an NTP server, click **Add**.

c. In the **Server IP Address** field, specify the NTP server IP address.

d. Click **Add**.

e. To change the list of NTP servers, click **Edit** or **Delete**.

f. Click **Next**.



7. In the **Email Setup** - Optional pane, perform the following actions:

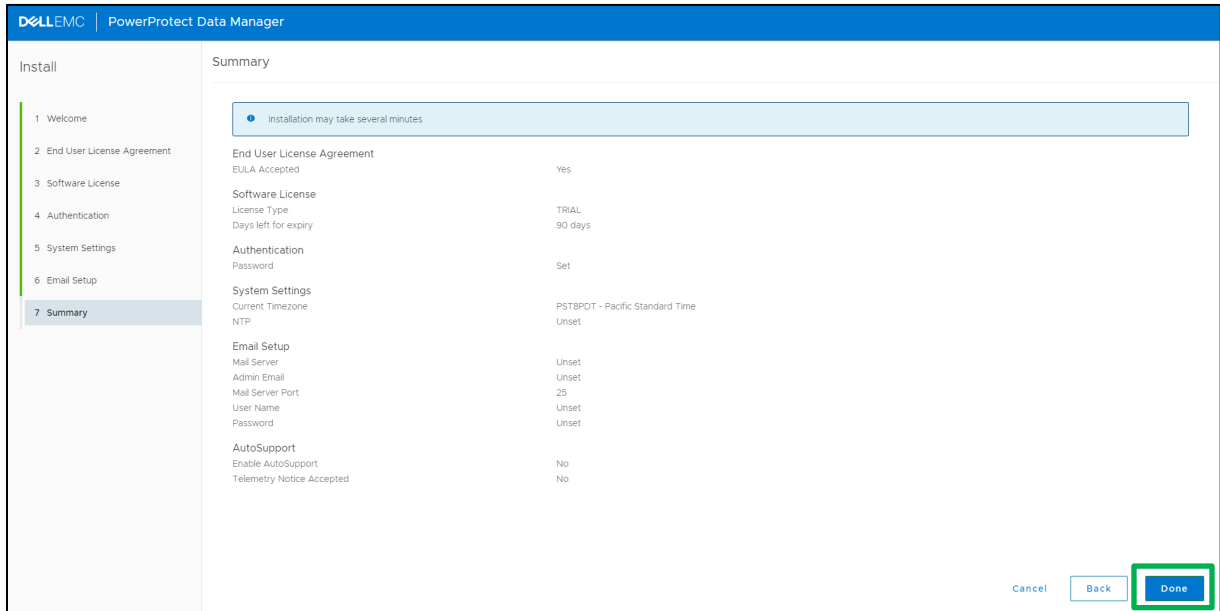
- a. In the **Mail Server** field, specify the SMTP server IP address.
- b. In the **Admin Email** field, specify the administrator email address.
- c. In the **Recipient for Test Email** field, specify the recipient email address.
- d. In the **Port** field, specify the TCP port to connect to the SMTP server.
- e. In the **Username** field, specify the mail username.
- f. In the **Password** field, specify the mail password.
- g. To send a test email to the specified IP address, click **Send Test Email**.
- h. To acknowledge the test email was successfully sent, click **OK**.
- i. To send diagnostic and usage data to Dell Technologies for proactive support and to help improve our products and services, switch **Auto Support** to **ON**.

When enabling auto support, click **View Terms** to review the telemetry software terms. Scroll down to click **Accept** to finish enabling auto support or **Decline** to disable auto support.

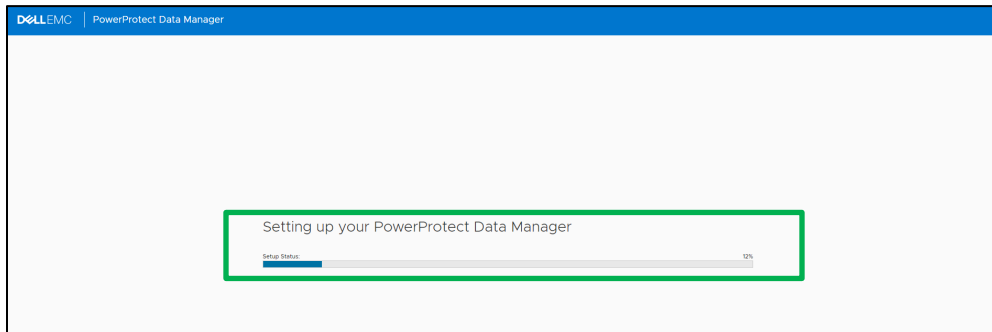
j. Click **Next**.

The screenshot displays the 'Email Setup' configuration screen in the Dell EMC PowerProtect Data Manager interface. The interface includes a sidebar on the left with a list of installation steps: 1 Welcome, 2 End User License Agreement, 3 Software License, 4 Authentication, 5 System Settings, 6 Email Setup (highlighted), 7 AutoSupport, and 8 Summary. The main content area is titled 'Email Setup' and contains a 'Configure Email' toggle switch (checked) with the note 'Required to enable AutoSupport'. Below this, the 'Server Settings' section includes several input fields: 'Mail Server' (placeholder: 'hostname or ip address', marked '(Required)'), 'Admin Email' (placeholder: 'administrator email', marked '(Required)'), 'Recipient for Test Email' (placeholder: 'recipient email', with a note 'Required in order to send a test email'), 'Port' (placeholder: '25'), 'User Name' (placeholder: 'user name'), and 'Password' (placeholder: 'password', with an eye icon for visibility). A 'Send Test Email' button is located below the password field. At the bottom right of the screen, there are three buttons: 'Cancel', 'Back', and 'Next' (highlighted with a green box).

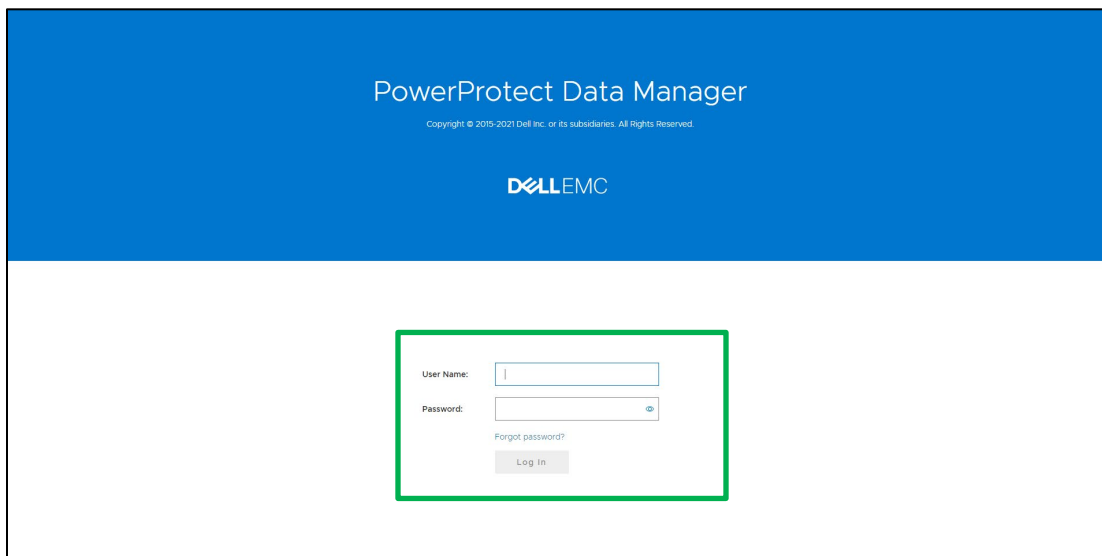
8. On the **Summary** pane, review the configuration choices and select **Done**.



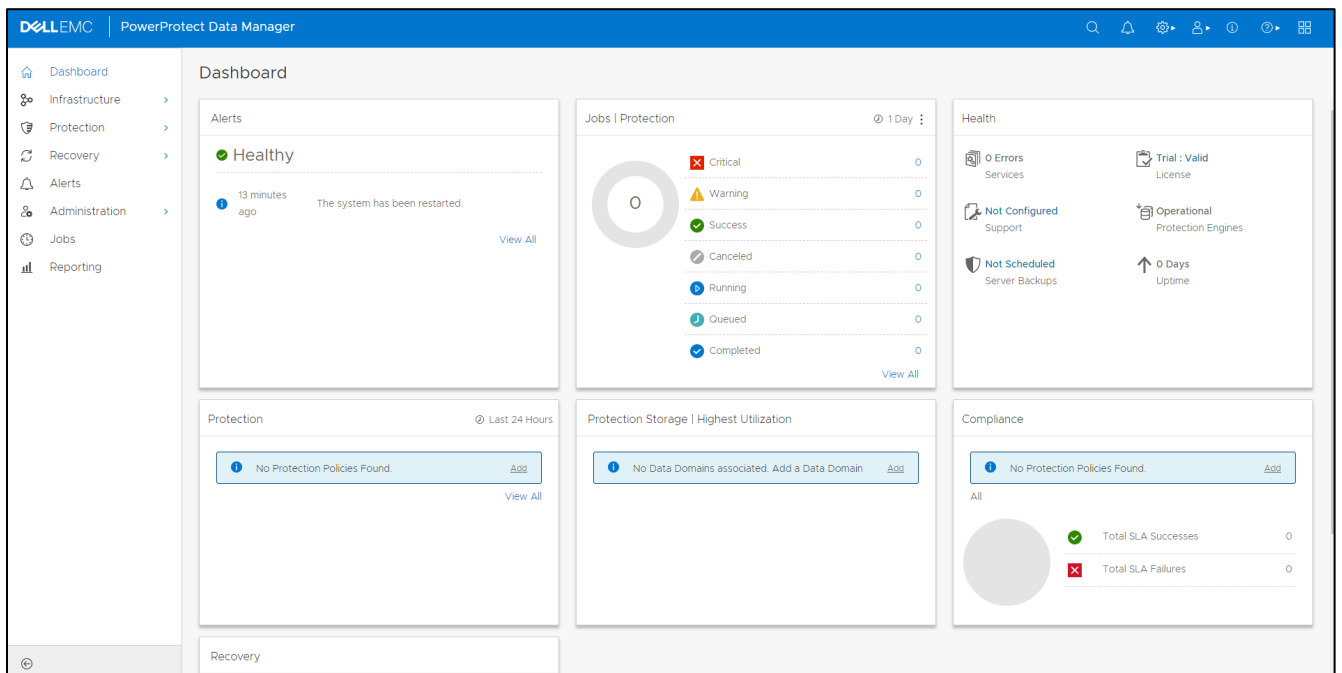
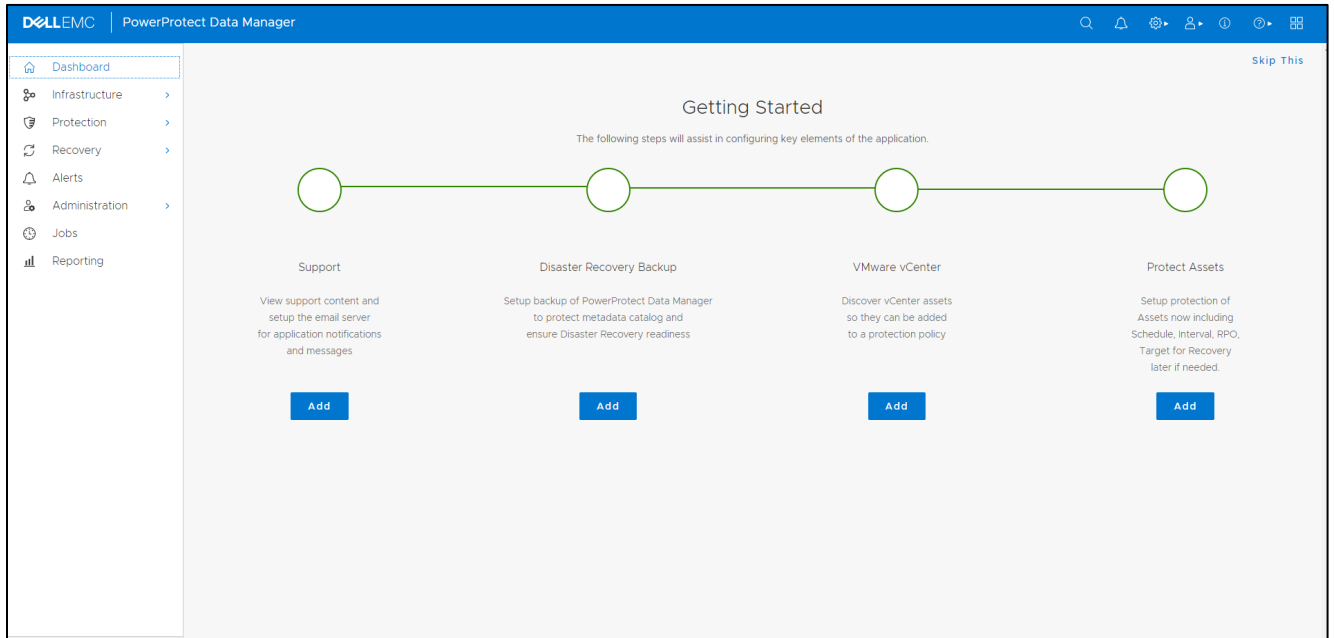
9. Within a few minutes, the Data Manager configuration is complete, and the login prompt appears.



10. Login with username as **admin** and use the password set during the configuration.



11. Data Manager is now ready to protect the cloud workloads running on Azure.



A Technical support and resources

[Dell.com/support](https://www.dell.com/support) is focused on meeting customer needs with proven services and support.

[Data Protection Info Hub](#) provides expertise that helps to ensure customer success with Dell EMC storage and data protection products.

A.1 Related resources

Dell EMC PowerProtect Data Manager

- [Dell EMC PowerProtect Data Manager Azure Deployment Guide](#)
- [Dell EMC PowerProtect Data Manager Administration and User Guide](#)
- [PowerProtect Data Manager Compatibility Matrix](#)

Dell EMC PowerProtect DD Virtual Edition

- [Dell EMC PowerProtect DDVE on Azure Installation and Administration Guide](#)