Technical White Paper

Dell EMC PowerProtect Data Manager: Deployment and configuration on Amazon Web Services

Next generation software platform for proven and modern cloud data protection

Abstract

This white paper explains on how to deploy and configure Dell EMC™ PowerProtect Data Manager on Amazon Web Services (AWS) for seamless protection of workloads on AWS cloud.

June 2021

Revisions

Date	Description
June 2021	Initial release

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.

Table of contents

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 save costs.

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

Data owners and administrators can deploy Data Manager with automation from the AWS 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 as well as cloud native applications running in Kubernetes containers. Data Manager along with Dell EMC PowerProtect DD Virtual Edition (DDVE) provide high level 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 AWS using Data Manager and DDVE.

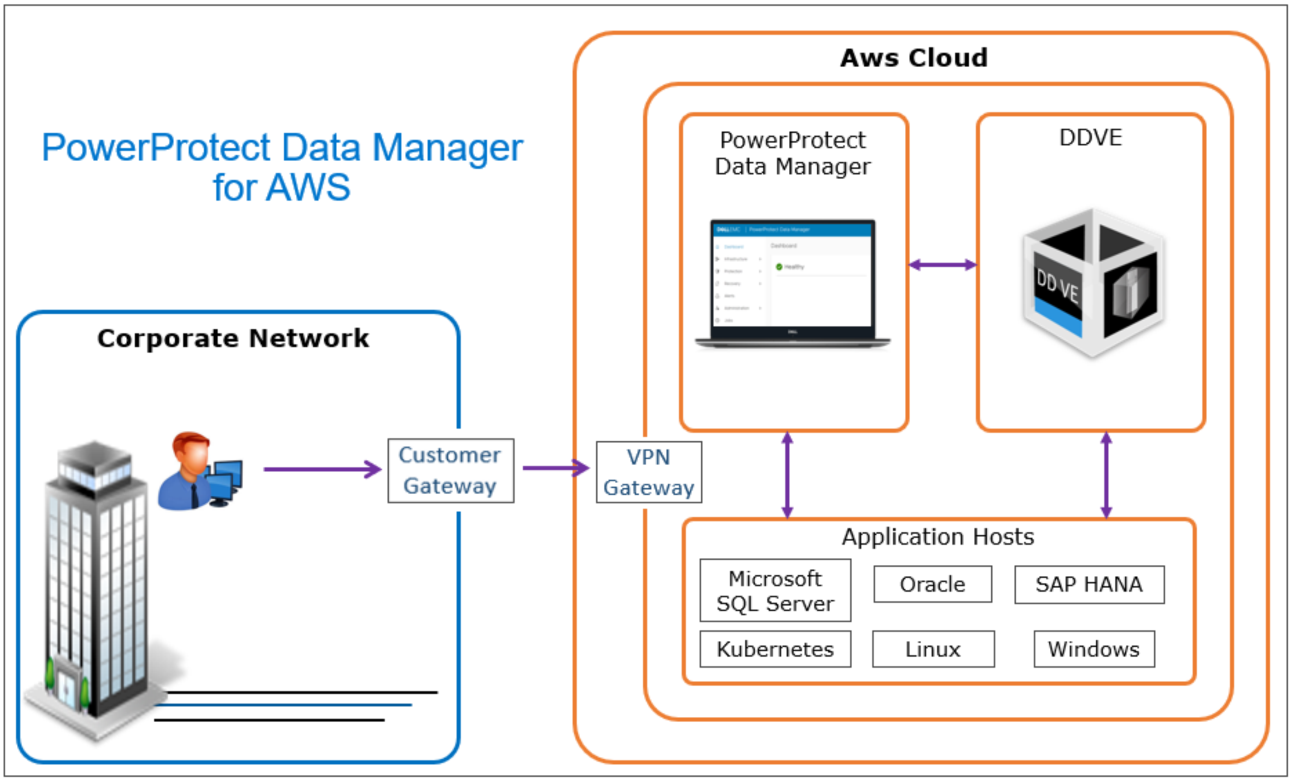
1 Introduction

1.1 Dell EMC PowerProtect Data Manager for AWS

Data Manager is a software-defined data protection software that can be installed in minutes on AWS cloud. Data Manager enables the transformation from traditional centralized protection to an IT-as-a-service model based on a self-service design.

Data Manager on AWS enables protection of traditional workloads including Oracle, SQL, SAP HANA, and file systems as well as cloud native applications running in Kubernetes containers or VMs running in VMware Cloud.

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

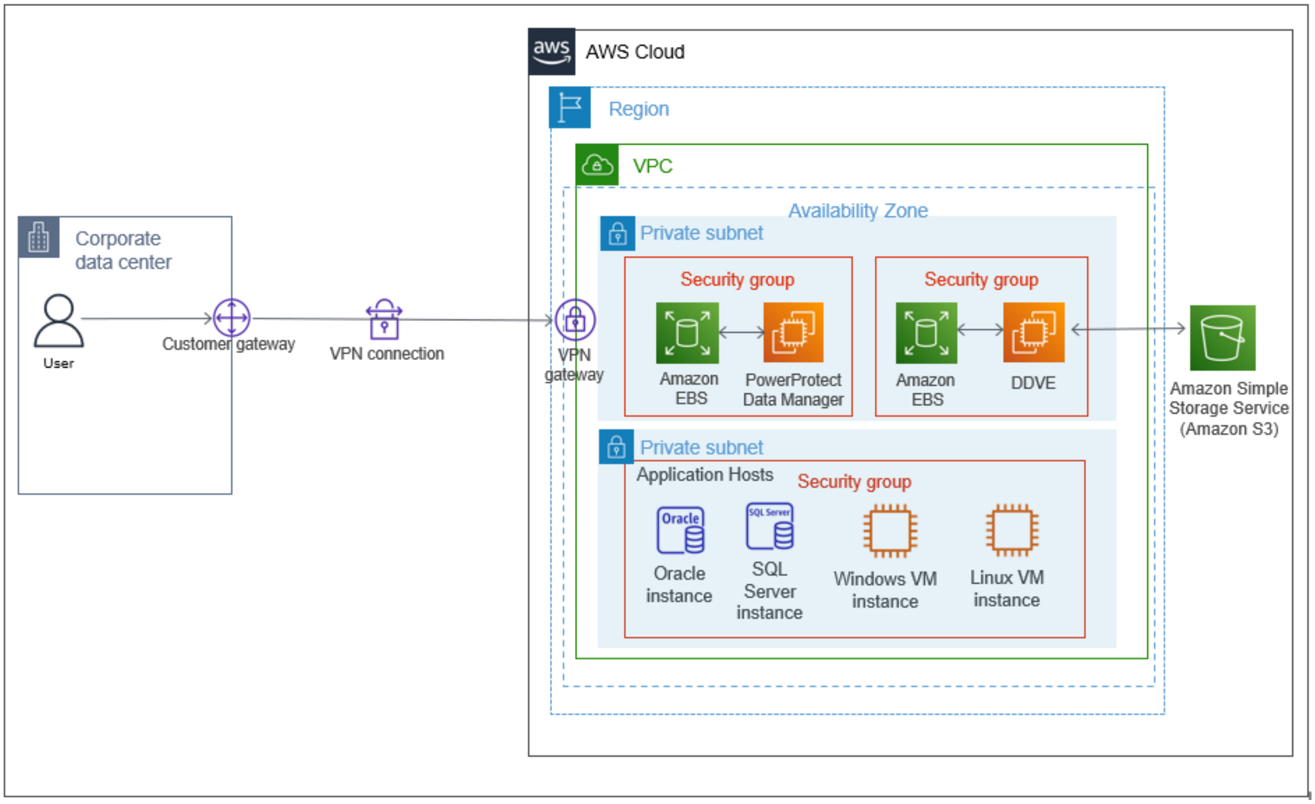


Using the AWS CloudFormation template, Data Manager can be deployed to an Elastic Compute Cloud (EC2) instance in a Virtual Private Cloud (VPC). Data Manager is deployed with a private IP address. A VPN gateway configuration is required to access Data Manager from an external site.

Data Manager deployed on AWS 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 AWS, the business-critical workloads deployed on AWS cloud can be protected.

1.2 Basic architecture overview

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



The Data Manager lockbox is in a secure Elastic Block Store (EBS) volume, where sensitive data, such as passwords, is encrypted and stored. Backup data is stored in a Simple Storage Services (S3) bucket, and the backup metadata is stored on a DDVE EBS volume.

Please see Dell EMC PowerProtect Data Manager Amazon Web Services Deployment Guide for more details on the different architecture models.

1.3 AWS data-transfer costs

Amazon charges the monthly fee based on the amount and types of data transferred by Data Manager and DDVE in AWS cloud.

- Most of the data that is transferred in an AWS cloud occurs between the hosts being protected and DDVE
- If Kubernetes is being used, data is also transferred between the protection engine hosts and DDVE
- Amazon does not have data-transfer fees for hosts that are in the same availability zone (AZ)

For pricing of Amazon monthly hosting in general, see the Amazon Pricing Calculator. For details on Amazon data-transfer fees, see Amazon EC2 Pricing

Note - To minimize data-transfer costs, minimize the path that data transfers take by using as few availability zones and regions as possible.

2 Deploying Data Manager and DDVE on AWS

2.1 Preparing for deployment

1. For a secure login to Data Manager, create an EC2 key access pair. See Amazon EC2 Key Pairs for instructions.
2. Set up the network environment. For secure access to the Data Manager on AWS, it is recommended to use the VPC architecture provided by AWS.

   Set up and configure the following components:
   - VPC
   - subnet
   - Route tables
   - Security groups
   - A network access control list
   - VPC Gateway endpoint for connectivity to S3

2.2 Deployment requirements

1. Create an AWS account. To set up an account, navigate to https://aws.amazon.com/getting-started/
2. As per AWS recommendation, create an identity and access management (IAM) user or role for authenticating with AWS and The IAM user must be allowed to perform AWS CloudFormation actions.
3. As a Security and operational best practices, Enable AWS CloudTrail logs to enable governance, compliance, and operational and risk auditing of AWS account.
4. IAM role that enables DDVE access to S3.
5. Empty S3 bucket name for automatic configuration.
6. Data Manager NTP server for Data Manager automatic configuration.
7. **VPC DNS requirements** - DNS resolution is critical for the deployment and configuration of the Data Manager external proxy and the Data Manager and DDVE appliances. Every infrastructure component should be resolvable through a fully qualified domain name (FQDN). Both forward (A) and reverse (PTR) lookups are required. When configuring VPC DNS, enable the following:
   - DNS resolution
   - DNS hostnames

   Note: DNS hostnames are disabled by default when a VPC is created.

See Dell EMC PowerProtect Data Manager Amazon Web Services Deployment Guide and Dell EMC PowerProtect DDVE on Amazon Web Services Installation and Administration Guide for more details on prerequisites for deploying Data Manager and DDVE on Azure.

2.3 Network interoperability

1. **VMware Cloud interoperability** - Data Manager for AWS supports all the features that are supported by VMC on AWS.
2. **DNS configuration** - If using a custom DNS server, a DNS server must be configured to be used for name resolution of hosts in the VMC-on-AWS and Data Manager-on-AWS networks. This server can be in either the VMC-on-AWS network or the Data Manager-on-AWS network.

Forward and reverse lookups are required for the following hosts:

- the Data Manager instance
- all DDVE instances
- the VM Direct protection engines
- vCenter and ESXi

Set this DNS server as the primary DNS server for the Data Manager instance once it has been deployed.

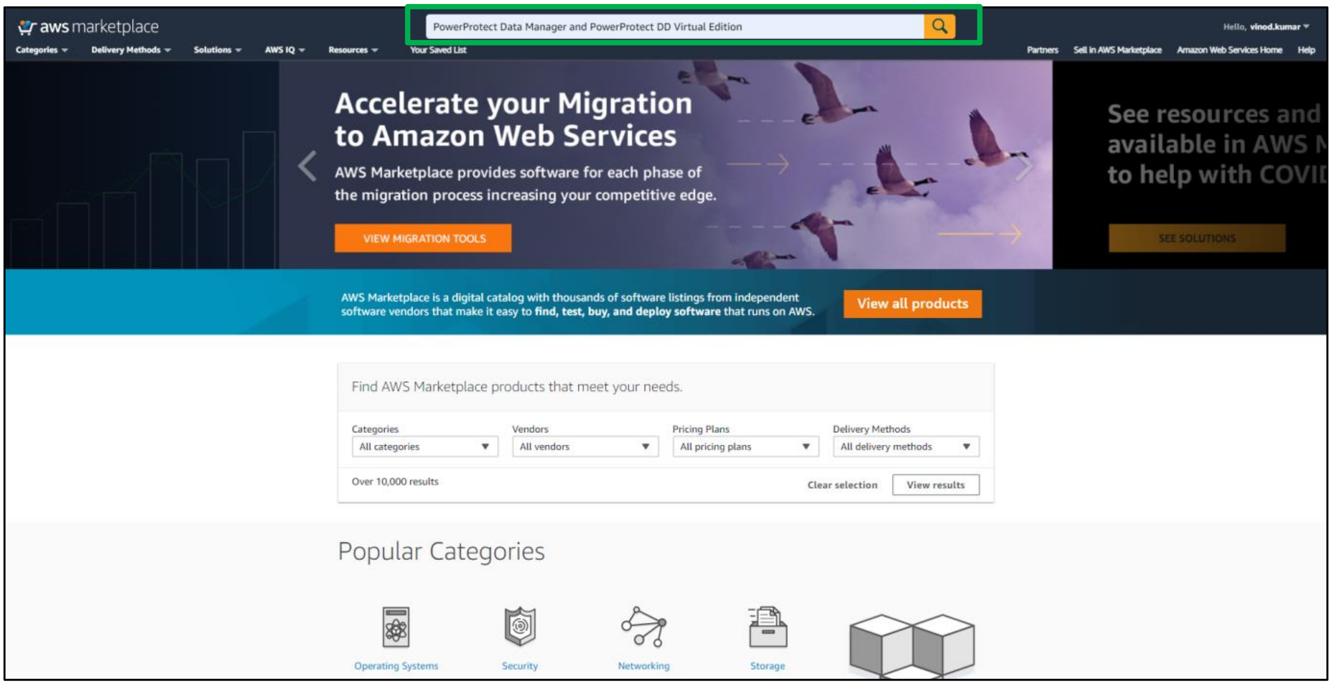
3. **Network traffic rules -** Network traffic rules must be configured for hosts in the Data Manager-on-AWS network to communicate with hosts in the VMC-on-AWS network.
   Data Manager requires inbound and outbound traffic between it and the following hosts in the VMC-on-AWS network:
   - the VM Direct protection engines
   - the primary DNS server
   - vCenter and ESXi

DDVE instance requires inbound and outbound traffic between them and the VM Direct protection engines in the VMC-on-AWS network. To configure DDVE traffic rules, see the PowerProtect Data Manager Administration and User Guide.

2.4 Steps to deploy Data Manager and DDVE on AWS

1. In a browser, navigate to https://aws.amazon.com/marketplace

2. Search for **PowerProtect Data Manager and PowerProtect DD Virtual Edition** in the search field.



PowerProtect Data Manager and PowerProtect DD Virtual Edition

Accelerate your Migration to Amazon Web Services

AWS Marketplace provides software for each phase of the migration process increasing your competitive edge.

See resources and available in AWS M to help with COVI

AWS Marketplace is a digital catalog with thousands of software listings from independent software vendors that make it easy to **find, test, buy, and deploy software** that runs on AWS.

Find AWS Marketplace products that meet your needs.

Categories: All categories

Vendors: All vendors

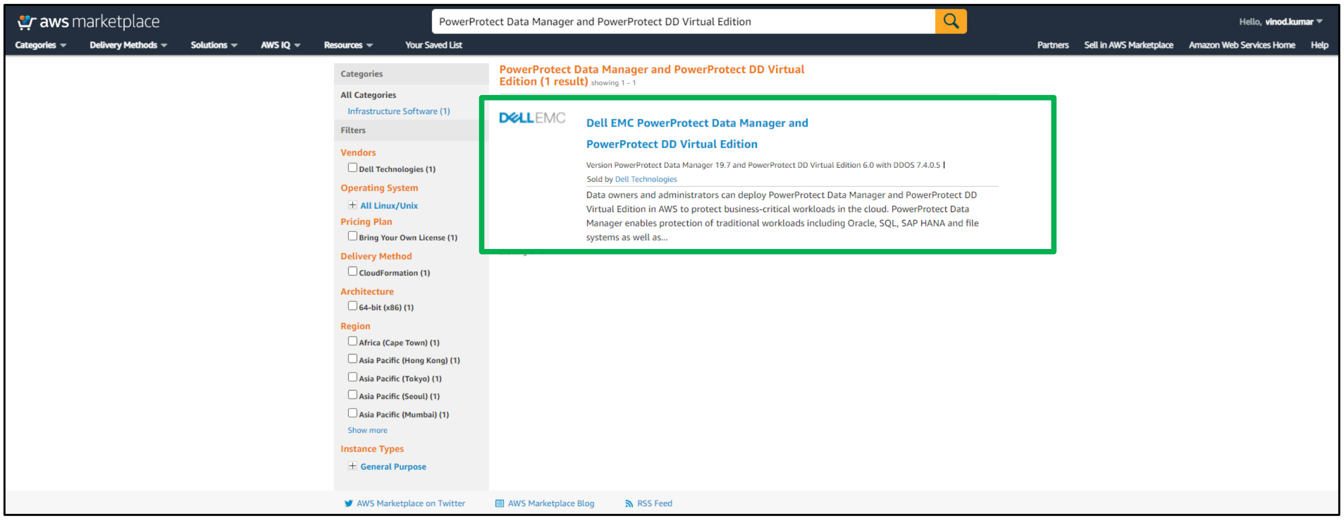
Pricing Plans: All pricing plans

Delivery Methods: All delivery methods

Over 10,000 results

Popular Categories

3. Select **Dell EMC PowerProtect Data Manager** and **PowerProtect DD Virtual Edition**.



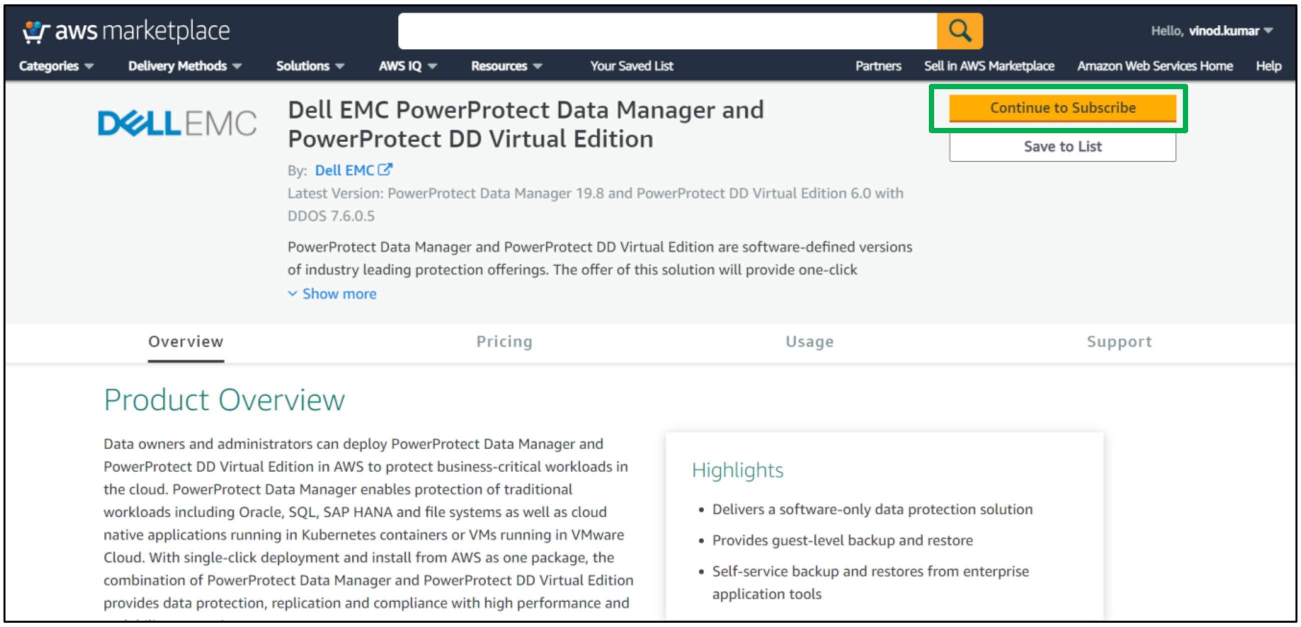
PowerProtect Data Manager and PowerProtect DD Virtual Edition (1 result) showing 1 - 1

Dell EMC PowerProtect Data Manager and PowerProtect DD Virtual Edition

Version PowerProtect Data Manager 19.7 and PowerProtect DD Virtual Edition 6.0 with DDOS 7.4.0.5 |
Sold by Dell Technologies

Data owners and administrators can deploy PowerProtect Data Manager and PowerProtect DD Virtual Edition in AWS to protect business-critical workloads in the cloud. PowerProtect Data Manager enables protection of traditional workloads including Oracle, SQL, SAP HANA and file systems as well as...

4. Select **Continue to Subscribe**.



Dell EMC PowerProtect Data Manager and PowerProtect DD Virtual Edition

By: Dell EMC

Latest Version: PowerProtect Data Manager 19.8 and PowerProtect DD Virtual Edition 6.0 with DDOS 7.6.0.5

PowerProtect Data Manager and PowerProtect DD Virtual Edition are software-defined versions of industry leading protection offerings. The offer of this solution will provide one-click

Show more

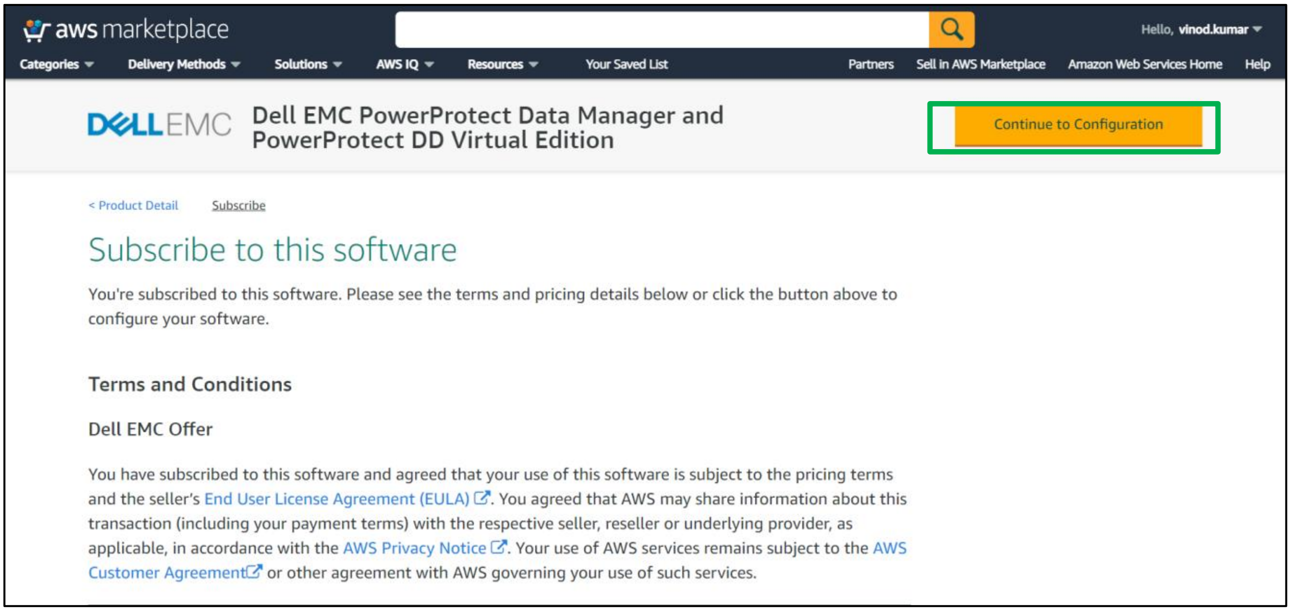
Product Overview

Data owners and administrators can deploy PowerProtect Data Manager and PowerProtect DD Virtual Edition in AWS to protect business-critical workloads in the cloud. PowerProtect Data Manager enables protection of traditional workloads including Oracle, SQL, SAP HANA and file systems as well as cloud native applications running in Kubernetes containers or VMs running in VMware Cloud. With single-click deployment and install from AWS as one package, the combination of PowerProtect Data Manager and PowerProtect DD Virtual Edition provides data protection, replication and compliance with high performance and

Highlights

- Delivers a software-only data protection solution
- Provides guest-level backup and restore
- Self-service backup and restores from enterprise application tools

5. Select **Continue to Configuration.**



Dell EMC PowerProtect Data Manager and PowerProtect DD Virtual Edition

Subscribe to this software

You're subscribed to this software. Please see the terms and pricing details below or click the button above to configure your software.

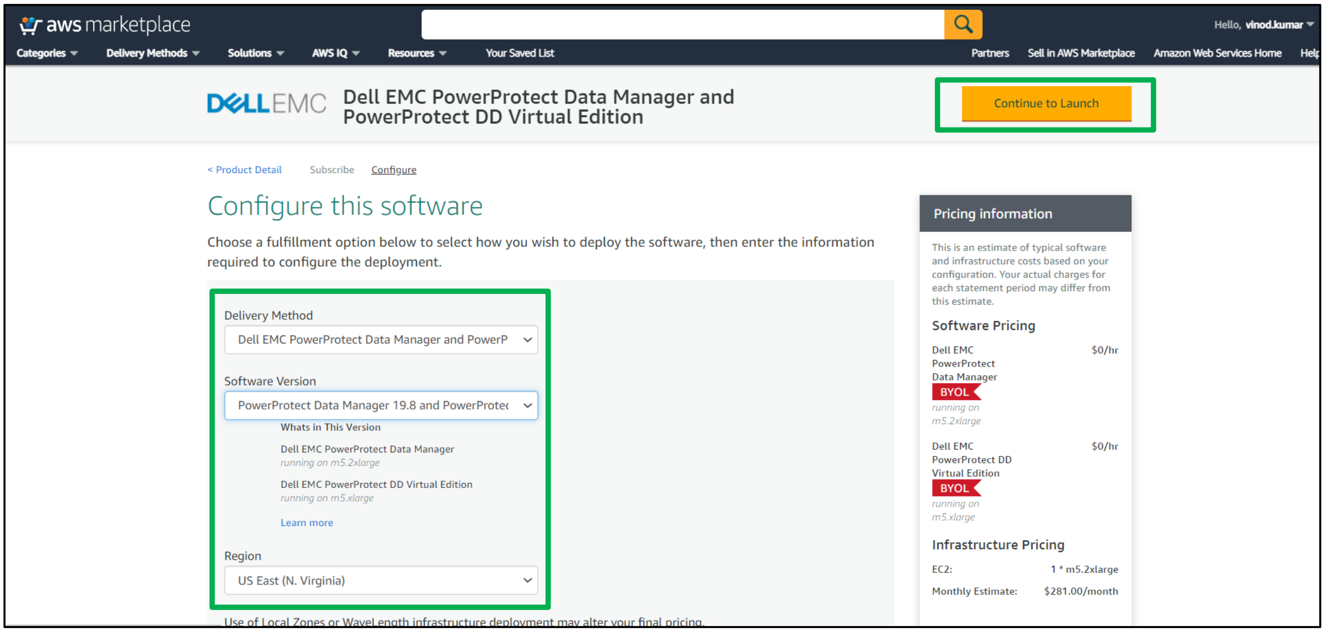
Terms and Conditions

Dell EMC Offer

You have subscribed to this software and agreed that your use of this software is subject to the pricing terms and the seller's End User License Agreement (EULA). You agreed that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the AWS Privacy Notice. Your use of AWS services remains subject to the AWS Customer Agreement or other agreement with AWS governing your use of such services.

6. Select the following configuration and choose **Continue to Launch**.

   – **Delivery Method** - Select the Cloud Formation Template
   – **Software Version -** Select the correct version
   – **Region -** Select where to deploy Data Manager and DDVE



Dell EMC PowerProtect Data Manager and PowerProtect DD Virtual Edition

Configure this software

Choose a fulfillment option below to select how you wish to deploy the software, then enter the information required to configure the deployment.

Delivery Method: Dell EMC PowerProtect Data Manager and PowerP

Software Version: PowerProtect Data Manager 19.8 and PowerProte(

Whats in This Version

Dell EMC PowerProtect Data Manager
running on m5.2xlarge

Dell EMC PowerProtect DD Virtual Edition
running on m5.xlarge

Region: US East (N. Virginia)

Use of Local Zones or WaveLength infrastructure deployment may alter your final pricing.

Pricing information

This is an estimate of typical software and infrastructure costs based on your configuration. Your actual charges for each statement period may differ from this estimate.

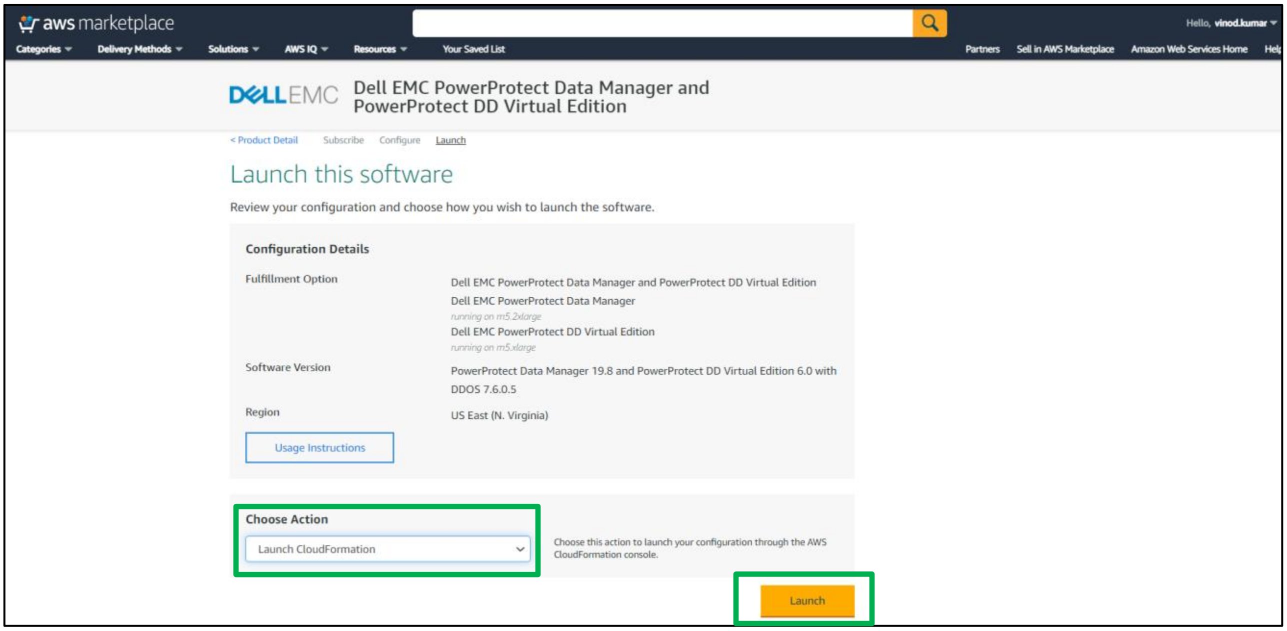
Software Pricing

Dell EMC PowerProtect Data Manager BYOL *running on m5.2xlarge*	$0/hr
Dell EMC PowerProtect DD Virtual Edition BYOL *running on m5.xlarge*	$0/hr

Infrastructure Pricing

EC2:	1 * m5.2xlarge
Monthly Estimate:	$281.00/month

7. Review the configuration details, Choose **Launch Cloud Formation** from **Choose Action** option and select **Launch**.



Dell EMC PowerProtect Data Manager and PowerProtect DD Virtual Edition

Launch this software

Review your configuration and choose how you wish to launch the software.

Configuration Details

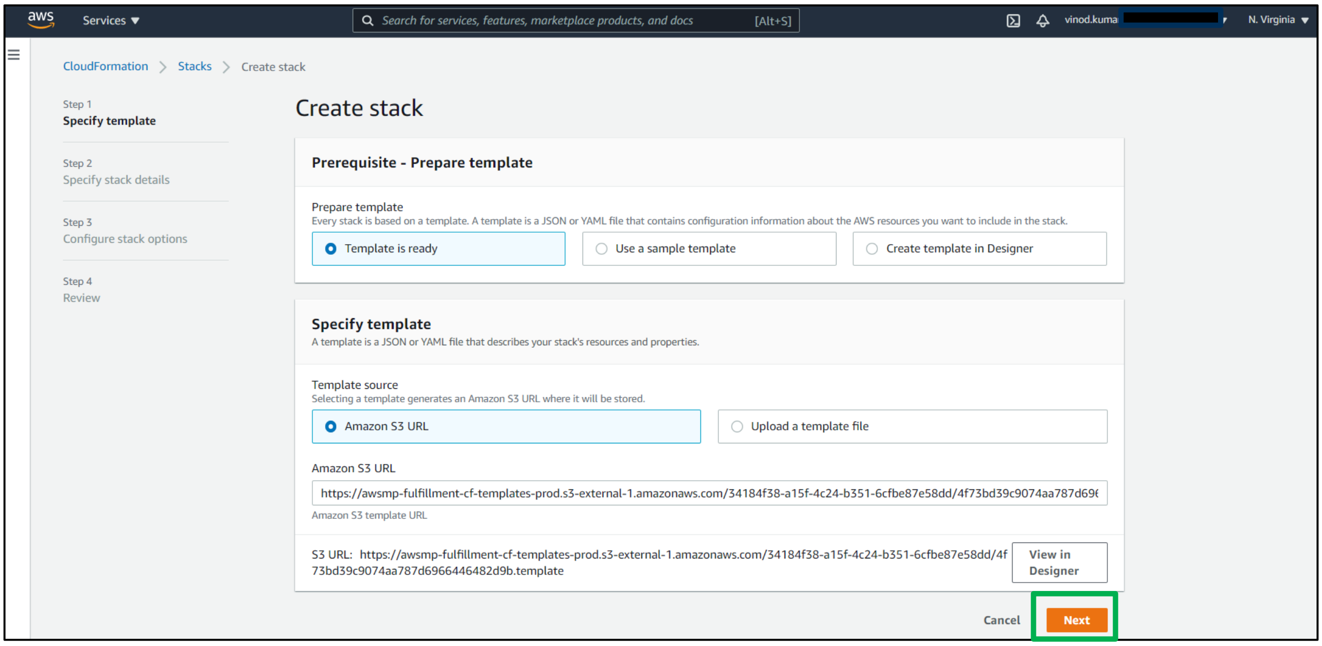
Fulfillment Option	Dell EMC PowerProtect Data Manager and PowerProtect DD Virtual Edition Dell EMC PowerProtect Data Manager *running on m5.2xlarge* Dell EMC PowerProtect DD Virtual Edition *running on m5.xlarge*
Software Version	PowerProtect Data Manager 19.8 and PowerProtect DD Virtual Edition 6.0 with DDOS 7.6.0.5
Region	US East (N. Virginia)

Choose Action

Launch CloudFormation

Choose this action to launch your configuration through the AWS CloudFormation console.

8. From the **CloudFormation** > **Stacks** > **Create stack** pane, click **Next**.



[redacted]

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Create stack

Prerequisite - Prepare template

Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

● Template is ready ○ Use a sample template ○ Create template in Designer

Specify template
A template is a JSON or YAML file that describes your stack's resources and properties.

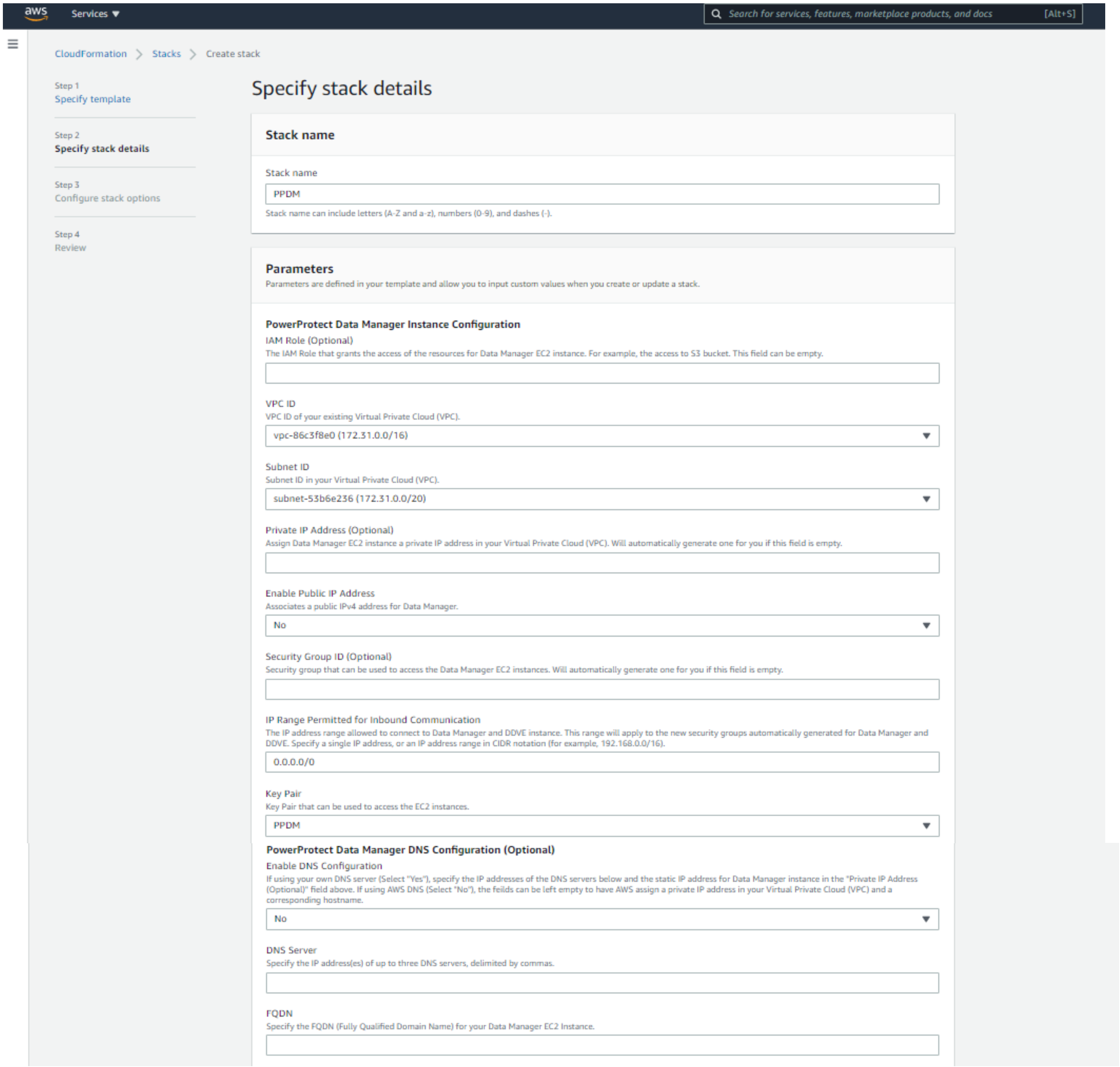
Template source
Selecting a template generates an Amazon S3 URL where it will be stored.

● Amazon S3 URL ○ Upload a template file

Amazon S3 URL
https://awsmp-fulfillment-cf-templates-prod.s3-external-1.amazonaws.com/34184f38-a15f-4c24-b351-6cfbe87e58dd/4f73bd39c9074aa787d69(
Amazon S3 template URL

S3 URL: https://awsmp-fulfillment-cf-templates-prod.s3-external-1.amazonaws.com/34184f38-a15f-4c24-b351-6cfbe87e58dd/4f73bd39c9074aa787d6966446482d9b.template

9. From the **CloudFormation > Stacks > Create stack > Specify stack details** pane, enter a name for the Data Manager in the Stack name text box and specify additional stack details and select **Next**.


aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
CloudFormation > Stacks > Create stack
Step 1
Specify template
Step 2
Specify stack details
Step 3
Configure stack options
Step 4
Review

Specify stack details

Stack name

Stack name

PPDM

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

PowerProtect Data Manager Instance Configuration

IAM Role (Optional)

The IAM Role that grants the access of the resources for Data Manager EC2 instance. For example, the access to S3 bucket. This field can be empty.

VPC ID

VPC ID of your existing Virtual Private Cloud (VPC).

vpc-86c3f8e0 (172.31.0.0/16) ▼

Subnet ID

Subnet ID in your Virtual Private Cloud (VPC).

subnet-53b6e236 (172.31.0.0/20) ▼

Private IP Address (Optional)

Assign Data Manager EC2 instance a private IP address in your Virtual Private Cloud (VPC). Will automatically generate one for you if this field is empty.

Enable Public IP Address

Associates a public IPv4 address for Data Manager.

No ▼

Security Group ID (Optional)

Security group that can be used to access the Data Manager EC2 instances. Will automatically generate one for you if this field is empty.

IP Range Permitted for Inbound Communication

The IP address range allowed to connect to Data Manager and DDVE instance. This range will apply to the new security groups automatically generated for Data Manager and DDVE. Specify a single IP address, or an IP address range in CIDR notation (for example, 192.168.0.0/16).

0.0.0.0/0

Key Pair

Key Pair that can be used to access the EC2 instances.

PPDM ▼

PowerProtect Data Manager DNS Configuration (Optional)

Enable DNS Configuration

If using your own DNS server (Select "Yes"), specify the IP addresses of the DNS servers below and the static IP address for Data Manager instance in the "Private IP Address (Optional)" field above. If using AWS DNS (Select "No"), the feilds can be left empty to have AWS assign a private IP address in your Virtual Private Cloud (VPC) and a corresponding hostname.

No ▼

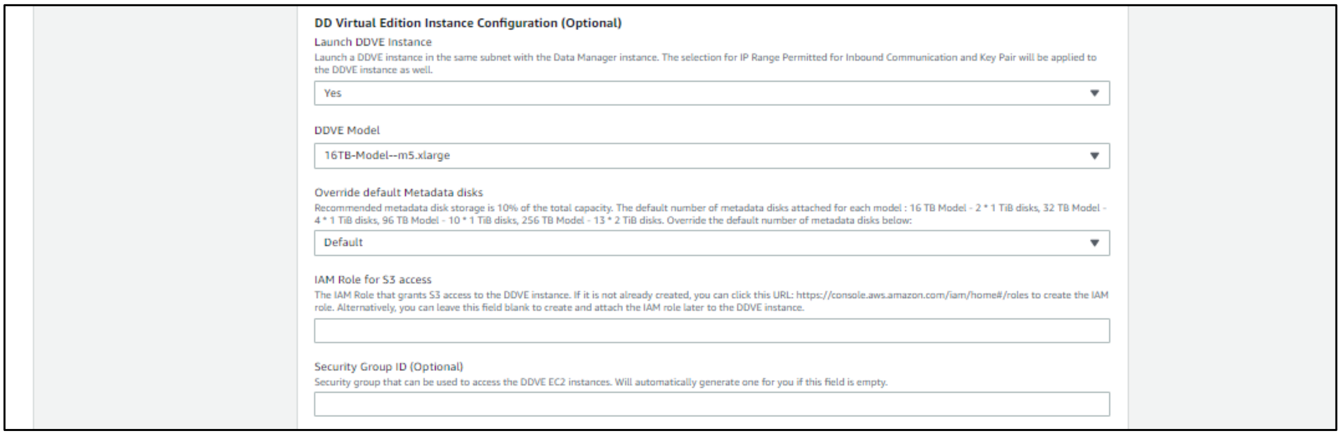
DNS Server

Specify the IP address(es) of up to three DNS servers, delimited by commas.

FQDN

Specify the FQDN (Fully Qualified Domain Name) for your Data Manager EC2 Instance.

DDVE instance configuration (Optional) - Select **Yes** to deploy and launch a DDVE instance in the same subnet as Data Manager. Enter the configuration settings that will be applied to the DDVE instance.



DD Virtual Edition Instance Configuration (Optional)

Launch DDVE Instance
Launch a DDVE instance in the same subnet with the Data Manager instance. The selection for IP Range Permitted for Inbound Communication and Key Pair will be applied to the DDVE instance as well.
Yes

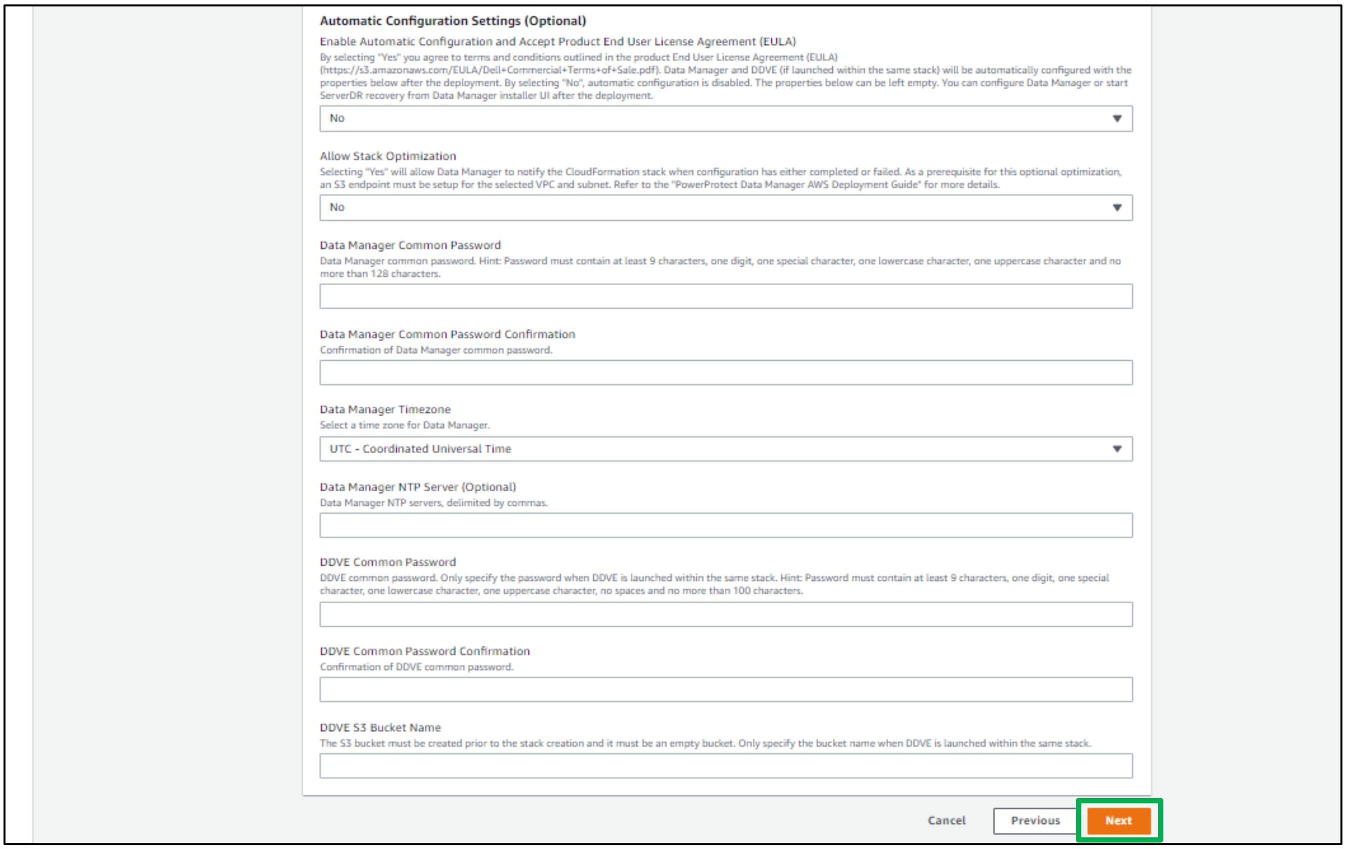
DDVE Model
16TB-Model--m5.xlarge

Override default Metadata disks
Recommended metadata disk storage is 10% of the total capacity. The default number of metadata disks attached for each model : 16 TB Model - 2 * 1 TiB disks, 32 TB Model - 4 * 1 TiB disks, 96 TB Model - 10 * 1 TiB disks, 256 TB Model - 13 * 2 TiB disks. Override the default number of metadata disks below:
Default

IAM Role for S3 access
The IAM Role that grants S3 access to the DDVE instance. If it is not already created, you can click this URL: https://console.aws.amazon.com/iam/home#/roles to create the IAM role. Alternatively, you can leave this field blank to create and attach the IAM role later to the DDVE instance.

Security Group ID (Optional)
Security group that can be used to access the DDVE EC2 instances. Will automatically generate one for you if this field is empty.

Data Manager automatic configuration (Optional) - Select **Yes** to enable **Automatic Configuration Settings** and to **Accept Product End User License Agreement (EULA)**. Enter the configuration settings that will be automatically applied to the Data Manager and DDVE instances when the stack is deployed.



Automatic Configuration Settings (Optional)

Enable Automatic Configuration and Accept Product End User License Agreement (EULA)
By selecting "Yes" you agree to terms and conditions outlined in the product End User License Agreement (EULA) (https://s3.amazonaws.com/EULA/Dell+Commercial+Terms+of+Sale.pdf). Data Manager and DDVE (if launched within the same stack) will be automatically configured with the properties below after the deployment. By selecting "No", automatic configuration is disabled. The properties below can be left empty. You can configure Data Manager or start ServerDR recovery from Data Manager installer UI after the deployment.
No

Allow Stack Optimization
Selecting "Yes" will allow Data Manager to notify the CloudFormation stack when configuration has either completed or failed. As a prerequisite for this optional optimization, an S3 endpoint must be setup for the selected VPC and subnet. Refer to the "PowerProtect Data Manager AWS Deployment Guide" for more details.
No

Data Manager Common Password
Data Manager common password. Hint: Password must contain at least 9 characters, one digit, one special character, one lowercase character, one uppercase character and no more than 128 characters.

Data Manager Common Password Confirmation
Confirmation of Data Manager common password.

Data Manager Timezone
Select a time zone for Data Manager.
UTC - Coordinated Universal Time

Data Manager NTP Server (Optional)
Data Manager NTP servers, delimited by commas.

DDVE Common Password
DDVE common password. Only specify the password when DDVE is launched within the same stack. Hint: Password must contain at least 9 characters, one digit, one special character, one lowercase character, one uppercase character, no spaces and no more than 100 characters.

DDVE Common Password Confirmation
Confirmation of DDVE common password.

DDVE S3 Bucket Name
The S3 bucket must be created prior to the stack creation and it must be an empty bucket. Only specify the bucket name when DDVE is launched within the same stack.

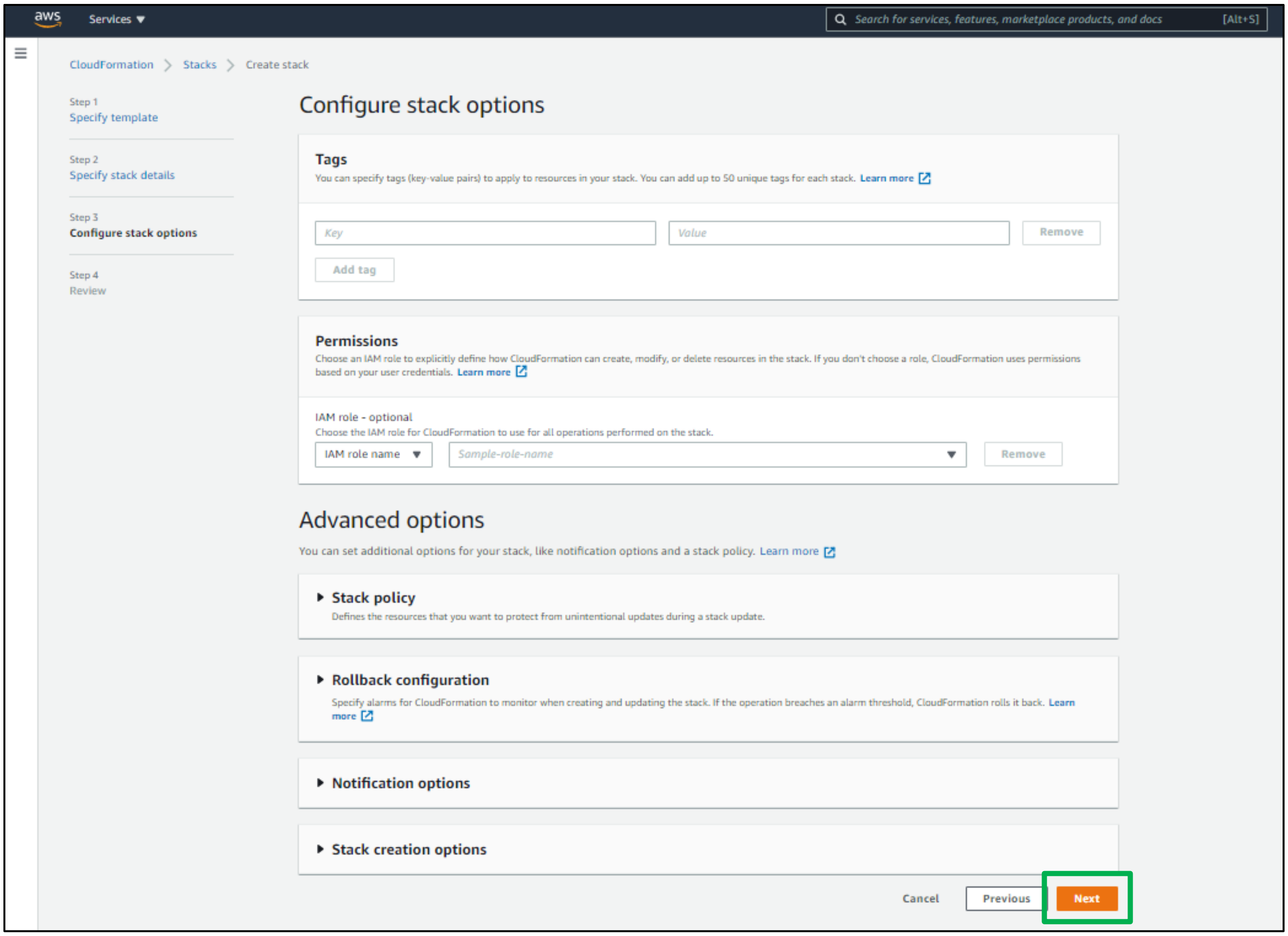
10. From the **CloudFormation > Stacks > Create stack > Configure stack options** page:

a. Either enable or disable **Rollback on failure**.

Note - Selecting Disabled is recommended.

- If Enabled, stack optimization was enabled, and automatic configuration was enabled but fails, then the deployment of Data Manager will be aborted
- If Disabled and automatic configuration was enabled but fails, then the instances must be manually configured after deployment

b. Click **Next**.



Configure stack options

Tags

You can specify tags (key-value pairs) to apply to resources in your stack. You can add up to 50 unique tags for each stack. Learn more

Permissions

Choose an IAM role to explicitly define how CloudFormation can create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses permissions based on your user credentials. Learn more

IAM role - optional

Choose the IAM role for CloudFormation to use for all operations performed on the stack.

Advanced options

You can set additional options for your stack, like notification options and a stack policy. Learn more

▸ Stack policy

Defines the resources that you want to protect from unintentional updates during a stack update.

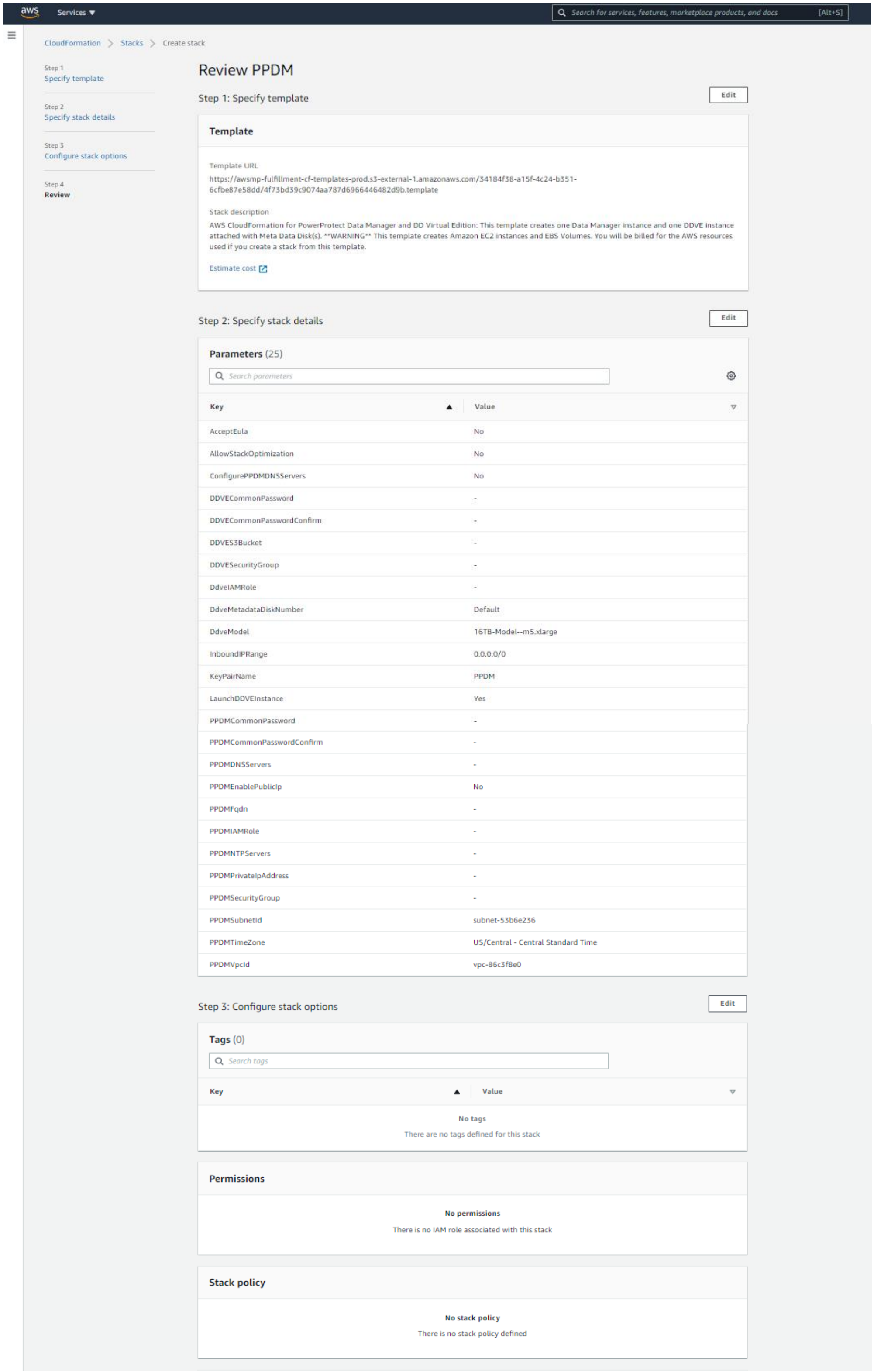
▸ Rollback configuration

Specify alarms for CloudFormation to monitor when creating and updating the stack. If the operation breaches an alarm threshold, CloudFormation rolls it back. Learn more

▸ Notification options

▸ Stack creation options

11. From the **CloudFormation > Stacks > Create stack > Review Stack Name** pane, review the information provided and Click **Create Stack** to create the Data Manager and DDVE instance.



Review PPDM

Step 1: Specify template

Template

Template URL
https://awsmp-fulfillment-cf-templates-prod.s3-external-1.amazonaws.com/34184f38-a15f-4c24-b351-6cfbe87e58dd/4f73bd39c9074aa787d6966446482d9b.template

Stack description
AWS CloudFormation for PowerProtect Data Manager and DD Virtual Edition: This template creates one Data Manager instance and one DDVE instance attached with Meta Data Disk(s). **WARNING** This template creates Amazon EC2 instances and EBS Volumes. You will be billed for the AWS resources used if you create a stack from this template.

Step 2: Specify stack details

Parameters (25)

Key ▲	Value ▽
AcceptEula	No
AllowStackOptimization	No
ConfigurePPDMDNSServers	No
DDVECommonPassword	-
DDVECommonPasswordConfirm	-
DDVES3Bucket	-
DDVESecurityGroup	-
DdveIAMRole	-
DdveMetadataDiskNumber	Default
DdveModel	16TB-Model--m5.xlarge
InboundIPRange	0.0.0.0/0
KeyPairName	PPDM
LaunchDDVEInstance	Yes
PPDMCommonPassword	-
PPDMCommonPasswordConfirm	-
PPDMDNSServers	-
PPDMEnablePublicIp	No
PPDMFqdn	-
PPDMIAMRole	-
PPDMNTPServers	-
PPDMPrivateIpAddress	-
PPDMSecurityGroup	-
PPDMSubnetId	subnet-53b6e236
PPDMTimeZone	US/Central - Central Standard Time
PPDMVpcId	vpc-86c3f8e0

Step 3: Configure stack options

Tags (0)

Key ▲	Value ▽

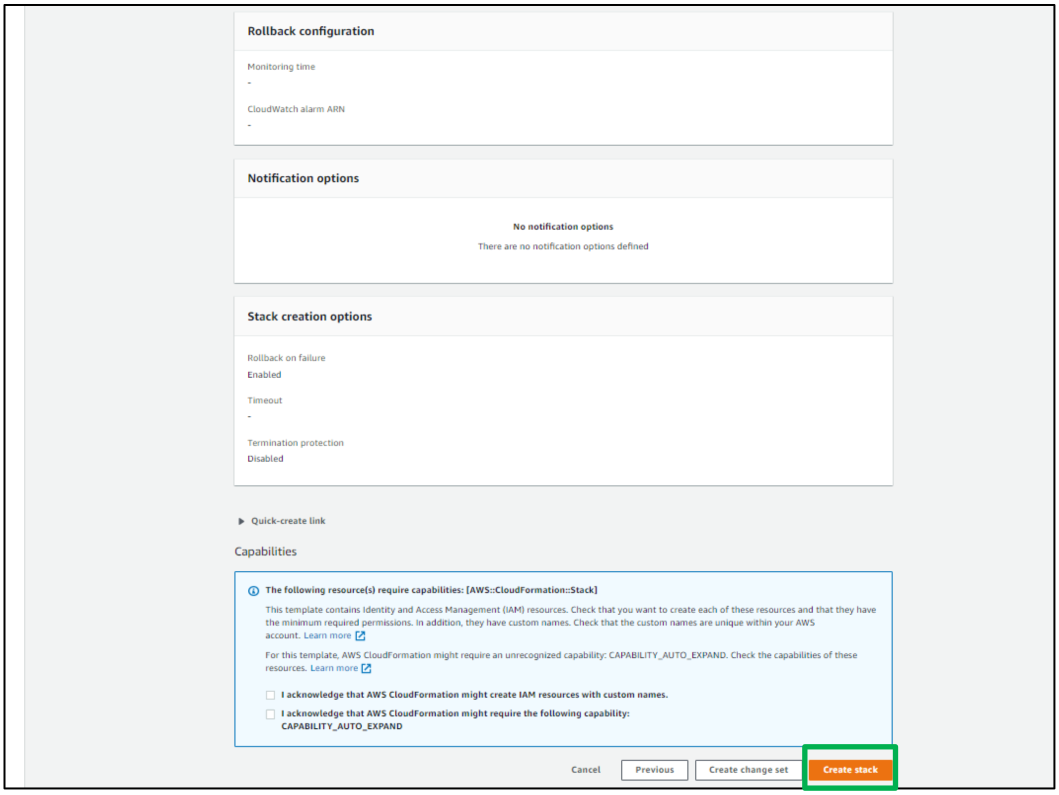
No tags
There are no tags defined for this stack

Permissions

No permissions
There is no IAM role associated with this stack

Stack policy

No stack policy
There is no stack policy defined



Rollback configuration

Monitoring time
-

CloudWatch alarm ARN
-

Notification options

No notification options

There are no notification options defined

Stack creation options

Rollback on failure
Enabled

Timeout
-

Termination protection
Disabled

▶ Quick-create link

Capabilities

ⓘ **The following resource(s) require capabilities: [AWS::CloudFormation::Stack]**

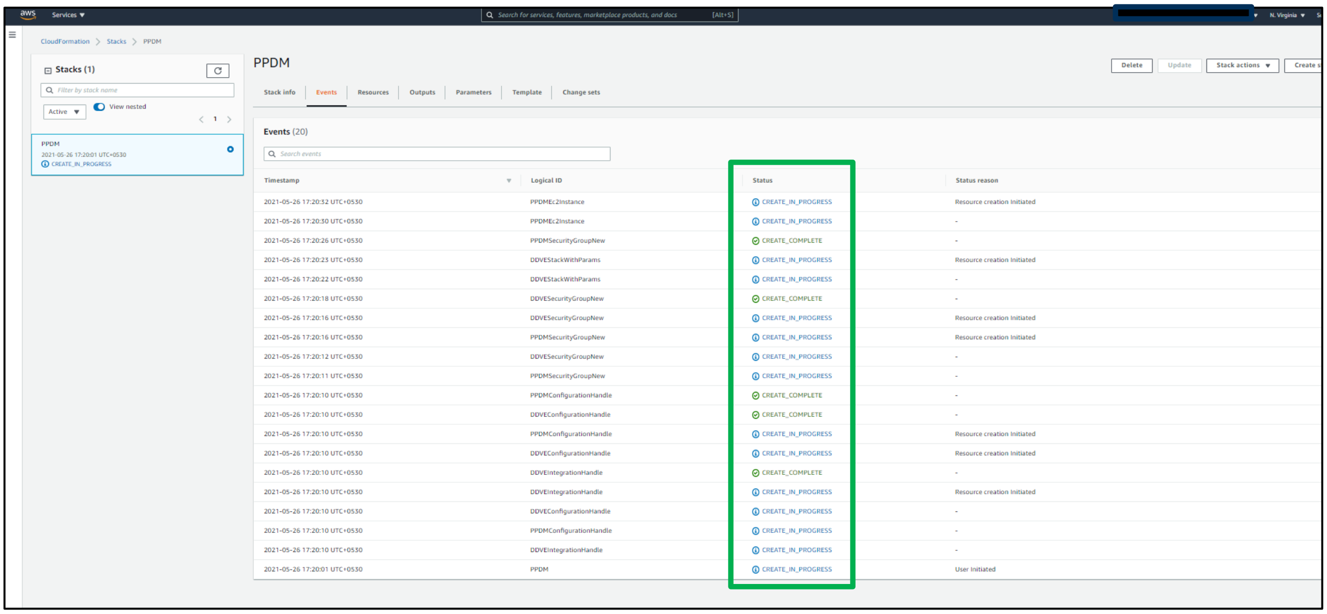
This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. Learn more

For this template, AWS CloudFormation might require an unrecognized capability: CAPABILITY_AUTO_EXPAND. Check the capabilities of these resources. Learn more

□ **I acknowledge that AWS CloudFormation might create IAM resources with custom names.**

□ **I acknowledge that AWS CloudFormation might require the following capability: CAPABILITY_AUTO_EXPAND**

12. Monitor the stack creation in progress and wait until **CREATE_COMPLETE** is displayed.



[redacted]

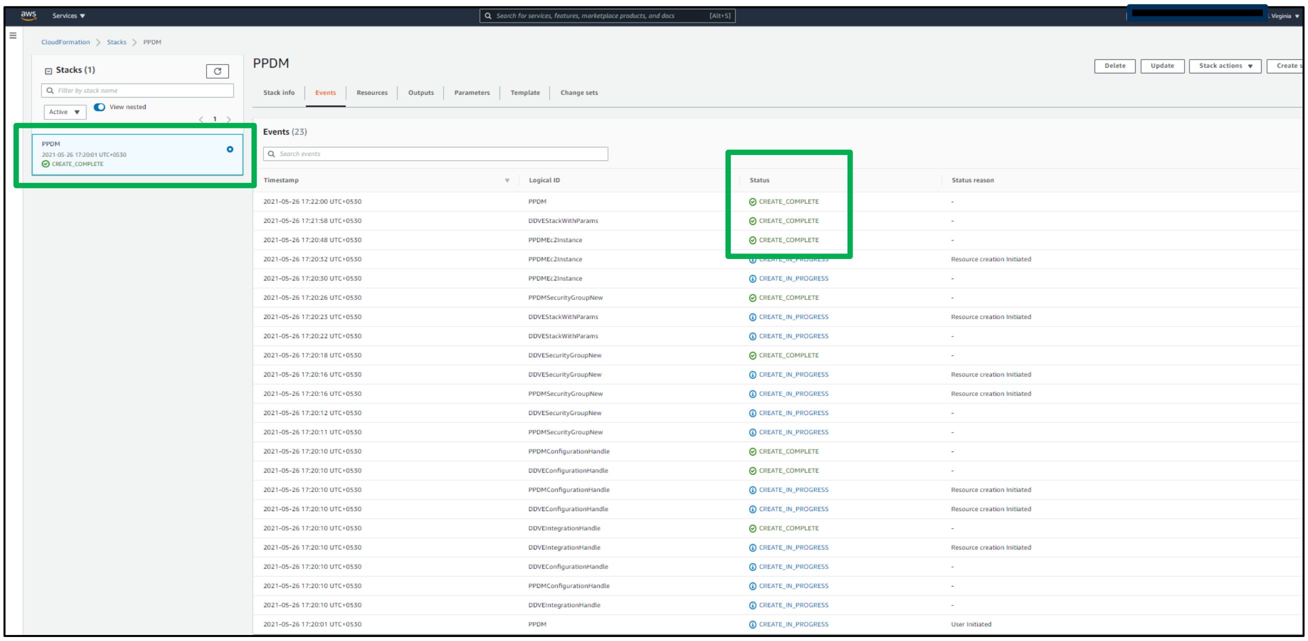
PPDM
2021-05-26 17:20:01 UTC+0530
ⓘ CREATE_IN_PROGRESS

PPDM

Events (20)

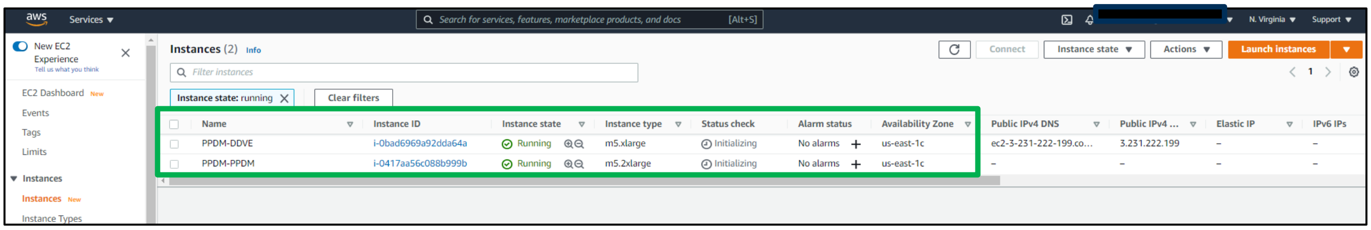
Timestamp	Logical ID	Status	Status reason
2021-05-26 17:20:32 UTC+0530	PPDMEc2Instance	ⓘ CREATE_IN_PROGRESS	Resource creation Initiated
2021-05-26 17:20:30 UTC+0530	PPDMEc2Instance	ⓘ CREATE_IN_PROGRESS	-
2021-05-26 17:20:26 UTC+0530	PPDMSecurityGroupNew	✓ CREATE_COMPLETE	-
2021-05-26 17:20:23 UTC+0530	DDVEStackWithParams	ⓘ CREATE_IN_PROGRESS	Resource creation Initiated
2021-05-26 17:20:22 UTC+0530	DDVEStackWithParams	ⓘ CREATE_IN_PROGRESS	-
2021-05-26 17:20:18 UTC+0530	DDVESecurityGroupNew	✓ CREATE_COMPLETE	-
2021-05-26 17:20:16 UTC+0530	DDVESecurityGroupNew	ⓘ CREATE_IN_PROGRESS	Resource creation Initiated
2021-05-26 17:20:16 UTC+0530	PPDMSecurityGroupNew	ⓘ CREATE_IN_PROGRESS	Resource creation Initiated
2021-05-26 17:20:12 UTC+0530	DDVESecurityGroupNew	ⓘ CREATE_IN_PROGRESS	-
2021-05-26 17:20:11 UTC+0530	PPDMSecurityGroupNew	ⓘ CREATE_IN_PROGRESS	-
2021-05-26 17:20:10 UTC+0530	PPDMConfigurationHandle	✓ CREATE_COMPLETE	-
2021-05-26 17:20:10 UTC+0530	DDVEConfigurationHandle	✓ CREATE_COMPLETE	-
2021-05-26 17:20:10 UTC+0530	PPDMConfigurationHandle	ⓘ CREATE_IN_PROGRESS	Resource creation Initiated
2021-05-26 17:20:10 UTC+0530	DDVEConfigurationHandle	ⓘ CREATE_IN_PROGRESS	Resource creation Initiated
2021-05-26 17:20:10 UTC+0530	DDVEIntegrationHandle	✓ CREATE_COMPLETE	-
2021-05-26 17:20:10 UTC+0530	DDVEIntegrationHandle	ⓘ CREATE_IN_PROGRESS	Resource creation Initiated
2021-05-26 17:20:10 UTC+0530	DDVEConfigurationHandle	ⓘ CREATE_IN_PROGRESS	-
2021-05-26 17:20:10 UTC+0530	PPDMConfigurationHandle	ⓘ CREATE_IN_PROGRESS	-
2021-05-26 17:20:10 UTC+0530	DDVEIntegrationHandle	ⓘ CREATE_IN_PROGRESS	-
2021-05-26 17:20:01 UTC+0530	PPDM	ⓘ CREATE_IN_PROGRESS	User Initiated

13. The Data Manager and DDVE instance has been successfully created using the Cloud Formation template.



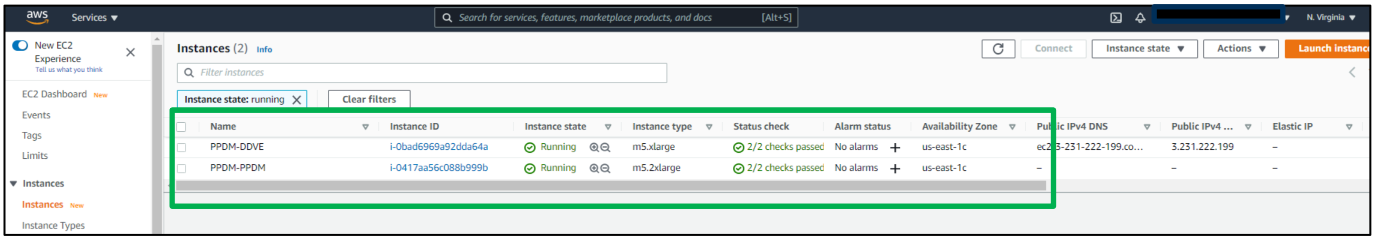
Timestamp	Logical ID	Status	Status reason
2021-05-26 17:22:00 UTC+0530	PPDM	CREATE_COMPLETE	-
2021-05-26 17:21:58 UTC+0530	DDVEStackWithParams	CREATE_COMPLETE	-
2021-05-26 17:20:48 UTC+0530	PPDMEc2Instance	CREATE_COMPLETE	-
2021-05-26 17:20:32 UTC+0530	PPDMEc2Instance	CREATE_IN_PROGRESS	Resource creation Initiated
2021-05-26 17:20:30 UTC+0530	PPDMEc2Instance	CREATE_IN_PROGRESS	-
2021-05-26 17:20:26 UTC+0530	PPDMSecurityGroupNew	CREATE_COMPLETE	-
2021-05-26 17:20:23 UTC+0530	DDVEStackWithParams	CREATE_IN_PROGRESS	Resource creation Initiated
2021-05-26 17:20:22 UTC+0530	DDVEStackWithParams	CREATE_IN_PROGRESS	-
2021-05-26 17:20:18 UTC+0530	DDVESecurityGroupNew	CREATE_COMPLETE	-
2021-05-26 17:20:16 UTC+0530	DDVESecurityGroupNew	CREATE_IN_PROGRESS	Resource creation Initiated
2021-05-26 17:20:16 UTC+0530	PPDMSecurityGroupNew	CREATE_IN_PROGRESS	Resource creation Initiated
2021-05-26 17:20:12 UTC+0530	DDVESecurityGroupNew	CREATE_IN_PROGRESS	-
2021-05-26 17:20:11 UTC+0530	PPDMSecurityGroupNew	CREATE_IN_PROGRESS	-
2021-05-26 17:20:10 UTC+0530	PPDMConfigurationHandle	CREATE_COMPLETE	-
2021-05-26 17:20:10 UTC+0530	DDVEConfigurationHandle	CREATE_COMPLETE	-
2021-05-26 17:20:10 UTC+0530	PPDMConfigurationHandle	CREATE_IN_PROGRESS	Resource creation Initiated
2021-05-26 17:20:10 UTC+0530	DDVEConfigurationHandle	CREATE_IN_PROGRESS	Resource creation Initiated
2021-05-26 17:20:10 UTC+0530	DDVEIntegrationHandle	CREATE_COMPLETE	-
2021-05-26 17:20:10 UTC+0530	DDVEIntegrationHandle	CREATE_IN_PROGRESS	Resource creation Initiated
2021-05-26 17:20:10 UTC+0530	DDVEConfigurationHandle	CREATE_IN_PROGRESS	-
2021-05-26 17:20:10 UTC+0530	PPDMConfigurationHandle	CREATE_IN_PROGRESS	-
2021-05-26 17:20:10 UTC+0530	DDVEIntegrationHandle	CREATE_IN_PROGRESS	-
2021-05-26 17:20:01 UTC+0530	PPDM	CREATE_IN_PROGRESS	User Initiated

14. From the EC2 Instance Management Console, wait until the Data Manager and DDVE instance are initialized and running.



□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs
□	PPDM-DDVE	i-0bad6969a92dda64a	Running	m5.xlarge	Initializing	No alarms +	us-east-1c	ec2-3-231-222-199.co...	3.231.222.199	–	–
□	PPDM-PPDM	i-0417aa56c088b999b	Running	m5.2xlarge	Initializing	No alarms +	us-east-1c	–	–	–	–

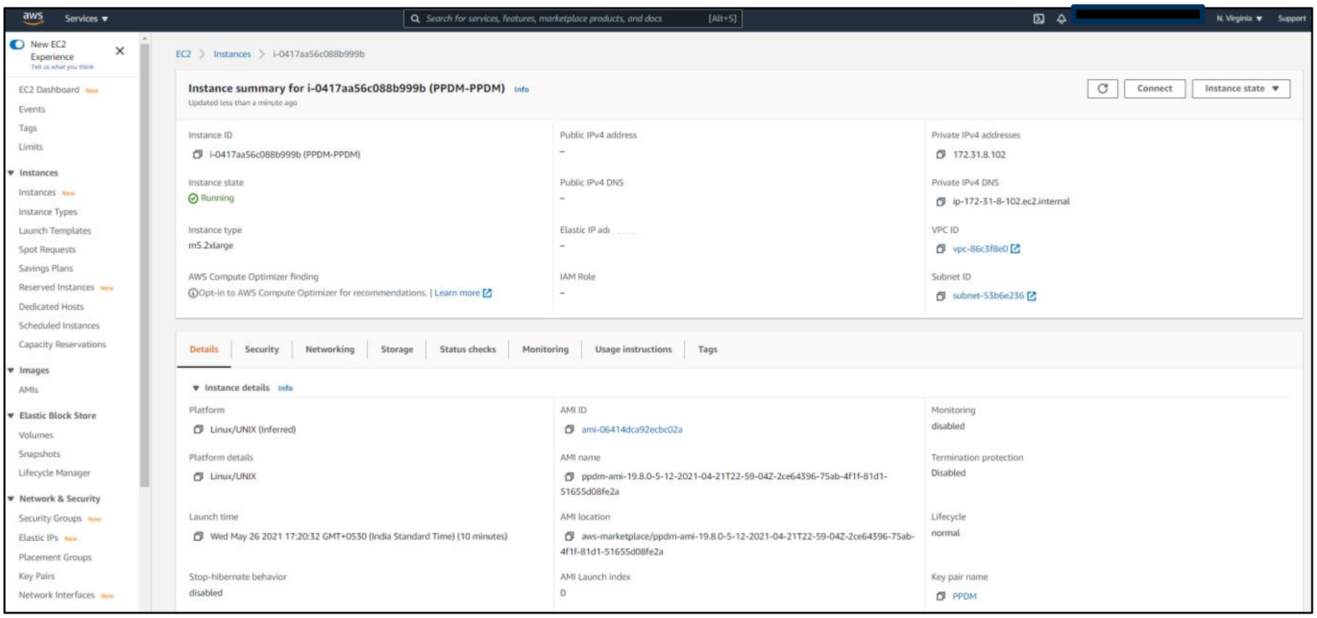
15. Data Manager and DDVE instance state are running and ready for configuration.



□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
□	PPDM-DDVE	i-0bad6969a92dda64a	Running	m5.xlarge	2/2 checks passed	No alarms +	us-east-1c	ec2-3-231-222-199.co...	3.231.222.199	–
□	PPDM-PPDM	i-0417aa56c088b999b	Running	m5.2xlarge	2/2 checks passed	No alarms +	us-east-1c	–	–	–

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

Data Manager instance is ready for configuration



Instance summary for i-0417aa56c088b999b (PPDM-PPDM) Info

Updated less than a minute ago

Instance ID: i-0417aa56c088b999b (PPDM-PPDM)

Instance state: Running

Instance type: m5.2xlarge

AWS Compute Optimizer finding: Opt-in to AWS Compute Optimizer for recommendations. | Learn more

Public IPv4 address: –

Public IPv4 DNS: –

Elastic IP adc: –

IAM Role: –

Private IPv4 addresses: 172.31.8.102

Private IPv4 DNS: ip-172-31-8-102.ec2.internal

VPC ID: vpc-86c3f8e0

Subnet ID: subnet-53b6e236

▾ Instance details Info

Platform: Linux/UNIX (Inferred)

Platform details: Linux/UNIX

Launch time: Wed May 26 2021 17:20:32 GMT+0530 (India Standard Time) (10 minutes)

Stop-hibernate behavior: disabled

AMI ID: ami-06414dca92ecbc02a

AMI name: ppdm-ami-19.8.0-5-12-2021-04-21T22-59-04Z-2ce64396-75ab-4f1f-81d1-51655d08fe2a

AMI location: aws-marketplace/ppdm-ami-19.8.0-5-12-2021-04-21T22-59-04Z-2ce64396-75ab-4f1f-81d1-51655d08fe2a

AMI Launch index: 0

Monitoring: disabled

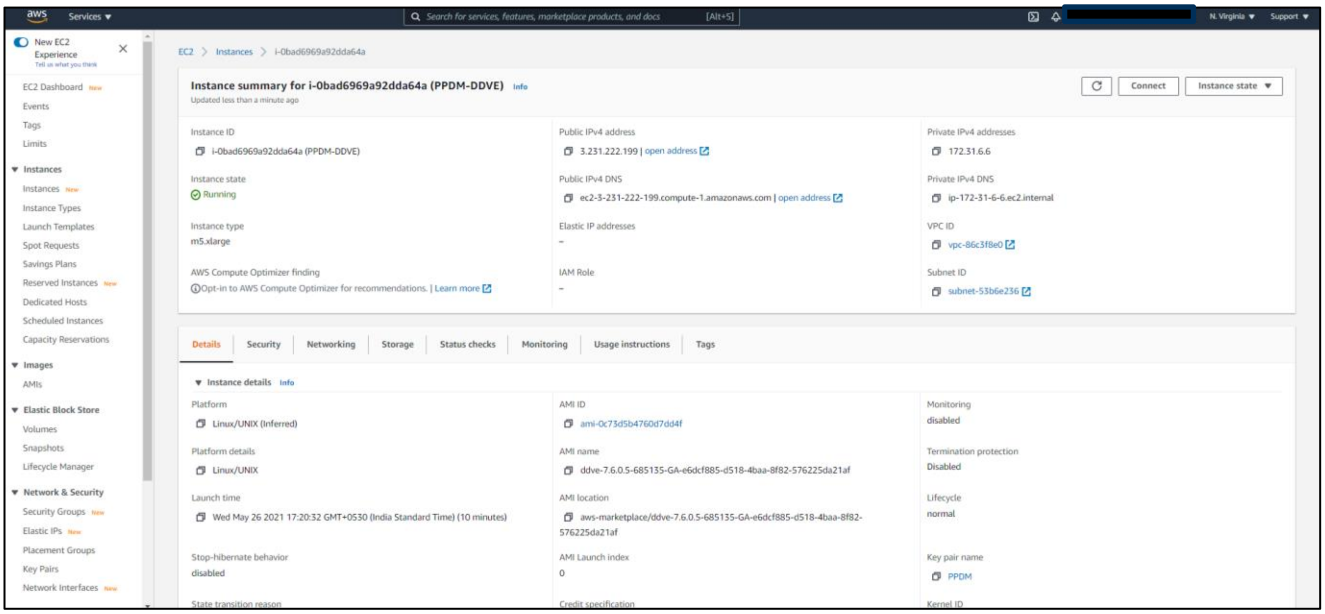
Termination protection: Disabled

Lifecycle: normal

Key pair name: PPDM

Refer Dell EMC PowerProtect Data Manager Amazon Web Services Deployment Guide for more detailed deployment information.

DDVE instance is ready for configuration



Instance summary for i-0bad6969a92dda64a (PPDM-DDVE) Info

Updated less than a minute ago

Instance ID: i-0bad6969a92dda64a (PPDM-DDVE)

Instance state: Running

Instance type: m5.xlarge

AWS Compute Optimizer finding: Opt-in to AWS Compute Optimizer for recommendations. | Learn more

Public IPv4 address: 3.231.222.199 | open address

Public IPv4 DNS: ec2-3-231-222-199.compute-1.amazonaws.com | open address

Elastic IP addresses: –

IAM Role: –

Private IPv4 addresses: 172.31.6.6

Private IPv4 DNS: ip-172-31-6-6.ec2.internal

VPC ID: vpc-86c3f8e0

Subnet ID: subnet-53b6e236

▾ Instance details Info

Platform: Linux/UNIX (Inferred)

Platform details: Linux/UNIX

Launch time: Wed May 26 2021 17:20:32 GMT+0530 (India Standard Time) (10 minutes)

Stop-hibernate behavior: disabled

State transition reason

AMI ID: ami-0c73d5b4760d7dd4f

AMI name: ddve-7.6.0.5-685135-GA-e6dcf885-d518-4baa-8f82-576225da21af

AMI location: aws-marketplace/ddve-7.6.0.5-685135-GA-e6dcf885-d518-4baa-8f82-576225da21af

AMI Launch index: 0

Credit specification

Monitoring: disabled

Termination protection: Disabled

Lifecycle: normal

Key pair name: PPDM

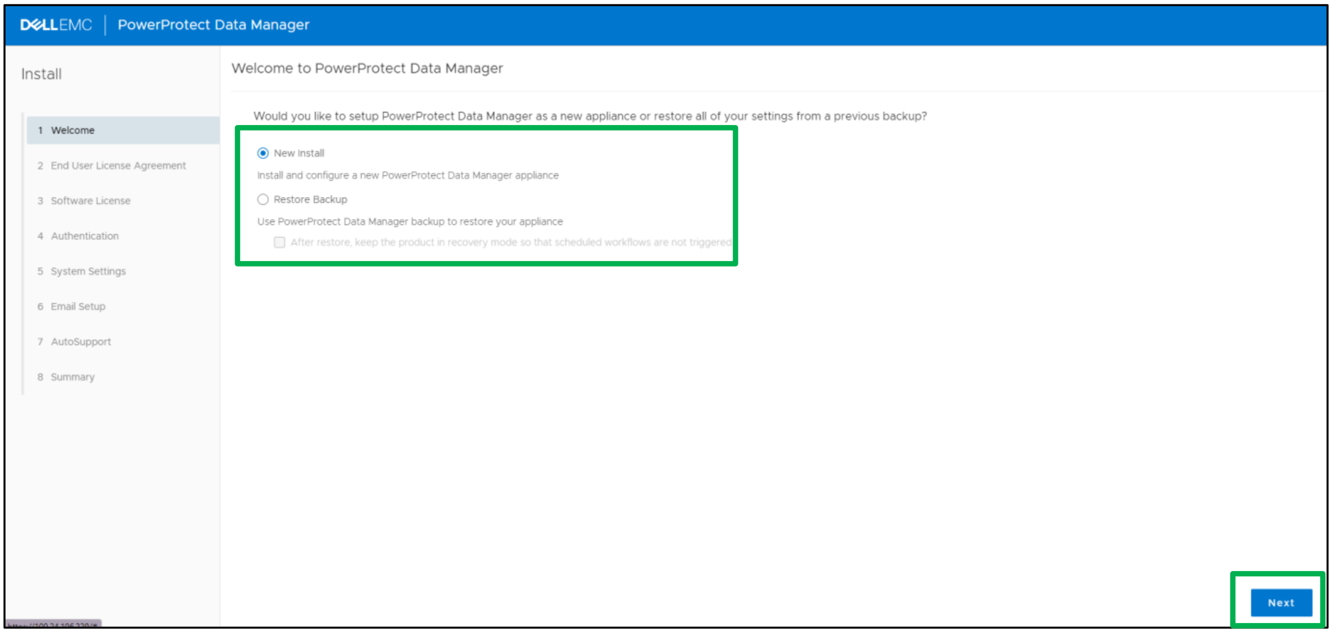
Kernel ID

Please see Dell EMC PowerProtect DDVE on Amazon Web Services Installation and Administration Guide for details on how to configure the DDVE instance deployed on AWS.

3 Configuring Data Manager deployed on AWS

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

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



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

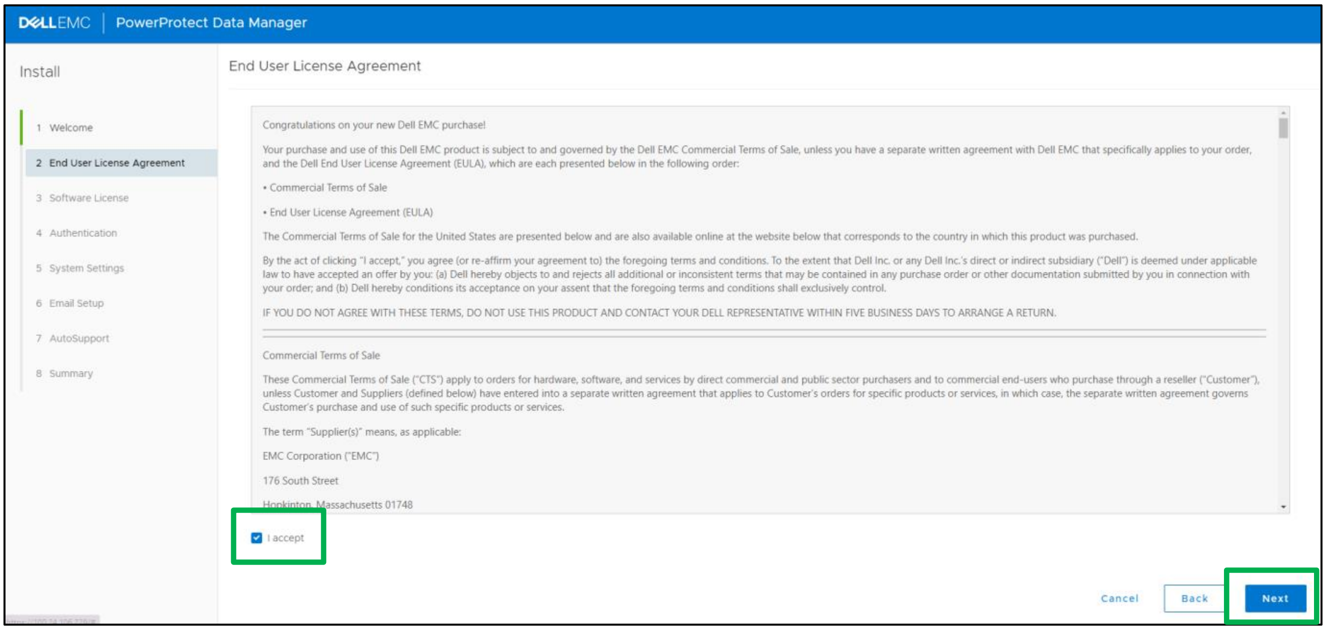
Install and configure a new PowerProtect Data Manager appliance

○ 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

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



End User License Agreement

Congratulations on your new Dell EMC purchase!

Your purchase and use of this Dell EMC product is subject to and governed by the Dell EMC Commercial Terms of Sale, unless you have a separate written agreement with Dell EMC that specifically applies to your order, and the Dell End User License Agreement (EULA), which are each presented below in the following order:

• Commercial Terms of Sale

• End User License Agreement (EULA)

The Commercial Terms of Sale for the United States are presented below and are also available online at the website below that corresponds to the country in which this product was purchased.

By the act of clicking "I accept," you agree (or re-affirm your agreement to) the foregoing terms and conditions. To the extent that Dell Inc. or any Dell Inc.'s direct or indirect subsidiary ("Dell") is deemed under applicable law to have accepted an offer by you: (a) Dell hereby objects to and rejects all additional or inconsistent terms that may be contained in any purchase order or other documentation submitted by you in connection with your order; and (b) Dell hereby conditions its acceptance on your assent that the foregoing terms and conditions shall exclusively control.

IF YOU DO NOT AGREE WITH THESE TERMS, DO NOT USE THIS PRODUCT AND CONTACT YOUR DELL REPRESENTATIVE WITHIN FIVE BUSINESS DAYS TO ARRANGE A RETURN.

Commercial Terms of Sale

These Commercial Terms of Sale ("CTS") apply to orders for hardware, software, and services by direct commercial and public sector purchasers and to commercial end-users who purchase through a reseller ("Customer"), unless Customer and Suppliers (defined below) have entered into a separate written agreement that applies to Customer's orders for specific products or services, in which case, the separate written agreement governs Customer's purchase and use of such specific products or services.

The term "Supplier(s)" means, as applicable:

EMC Corporation ("EMC")

176 South Street

Hopkinton, Massachusetts 01748

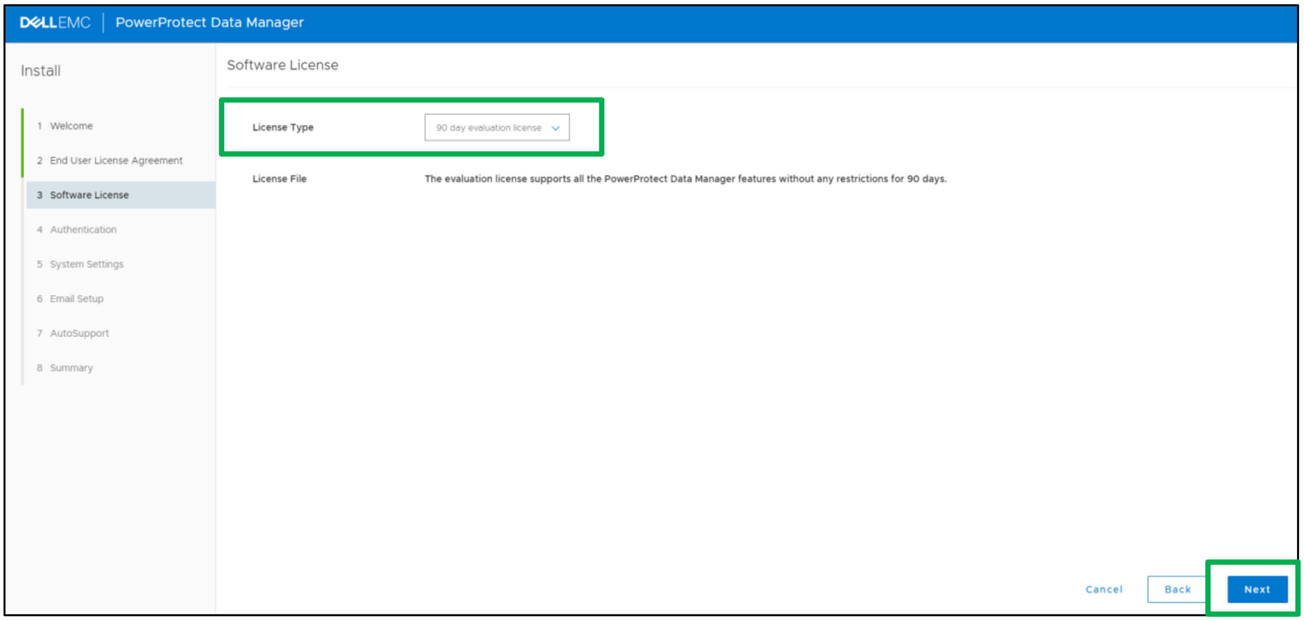
☑ I accept

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**.



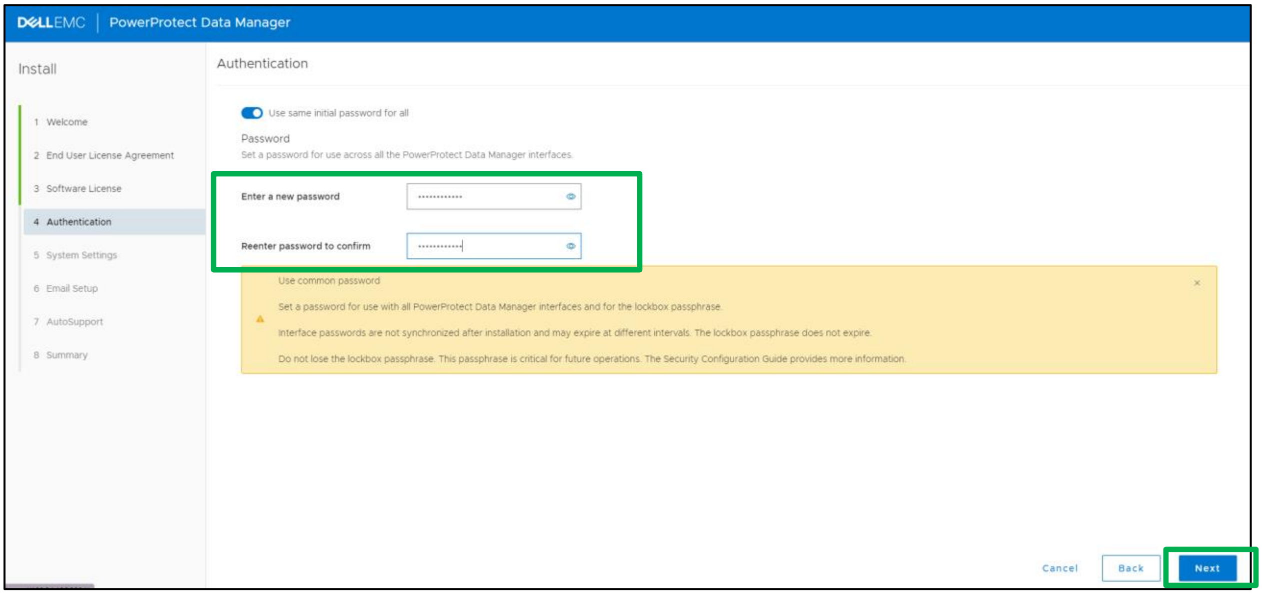
Software License

License Type: 90 day evaluation license

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

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.



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: ••••••••••••

Use common password

Set a password for use with all PowerProtect Data Manager interfaces and for the lockbox passphrase.

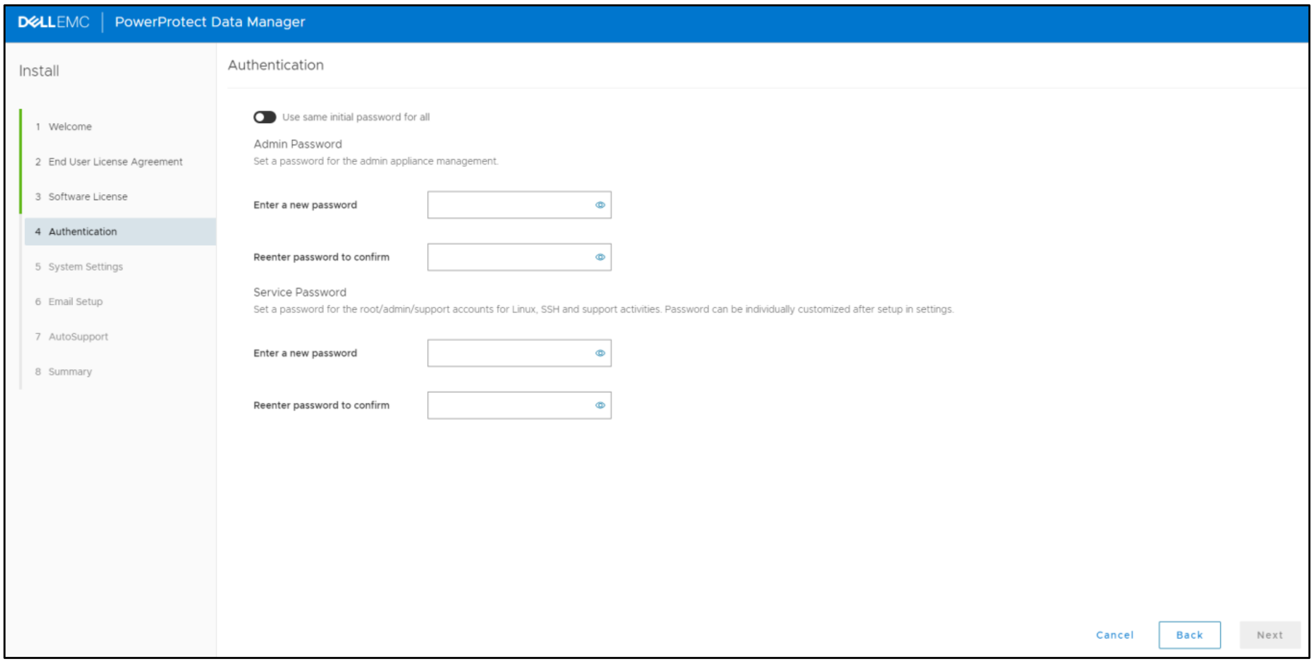
Interface passwords are not synchronized after installation and may expire at different intervals. The lockbox passphrase does not expire.

Do not lose the lockbox passphrase. This passphrase is critical for future operations. The Security Configuration Guide provides more information.

a. Optionally, clear the Use common password option.

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

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



Authentication

○ Use same initial password for all

Admin Password

Set a password for the admin appliance management.

Enter a new password

Reenter password to confirm

Service Password

Set a password for the root/admin/support accounts for Linux, SSH and support activities. Password can be individually customized after setup in settings.

Enter a new password

Reenter password to confirm

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.

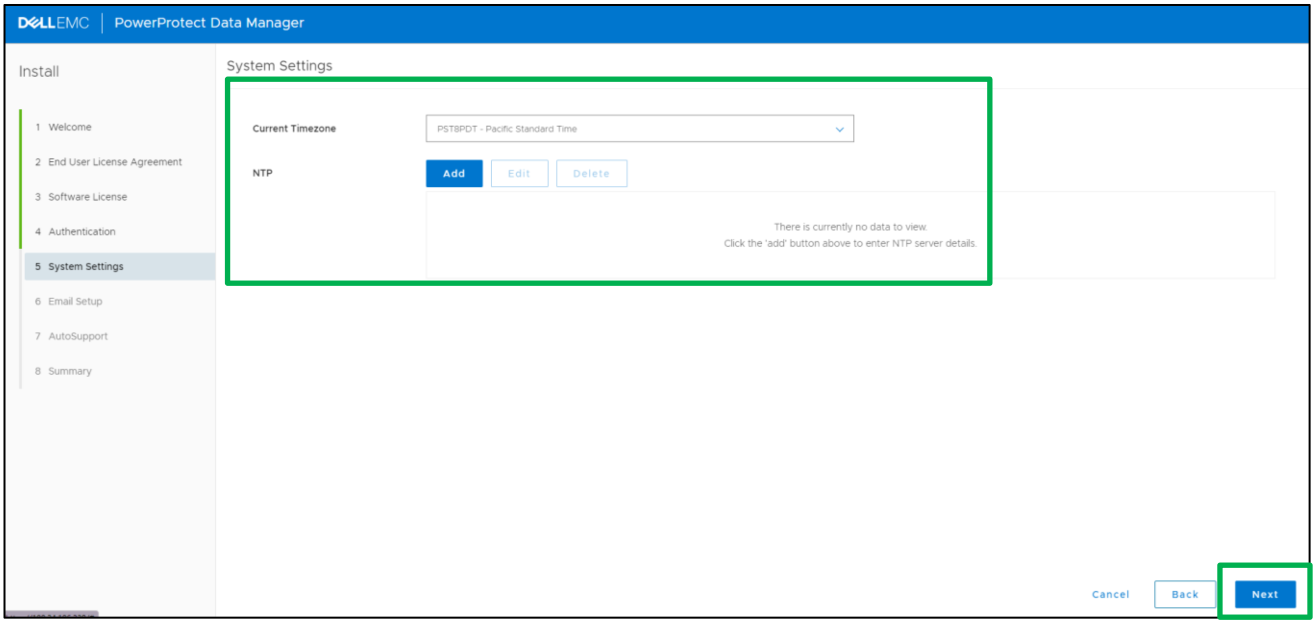
   b. To add an NTP server, click **Add**.

   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**.



System Settings

Current Timezone: PST8PDT - Pacific Standard Time

NTP

There is currently no data to view.
Click the 'add' button above to enter NTP server details.

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.

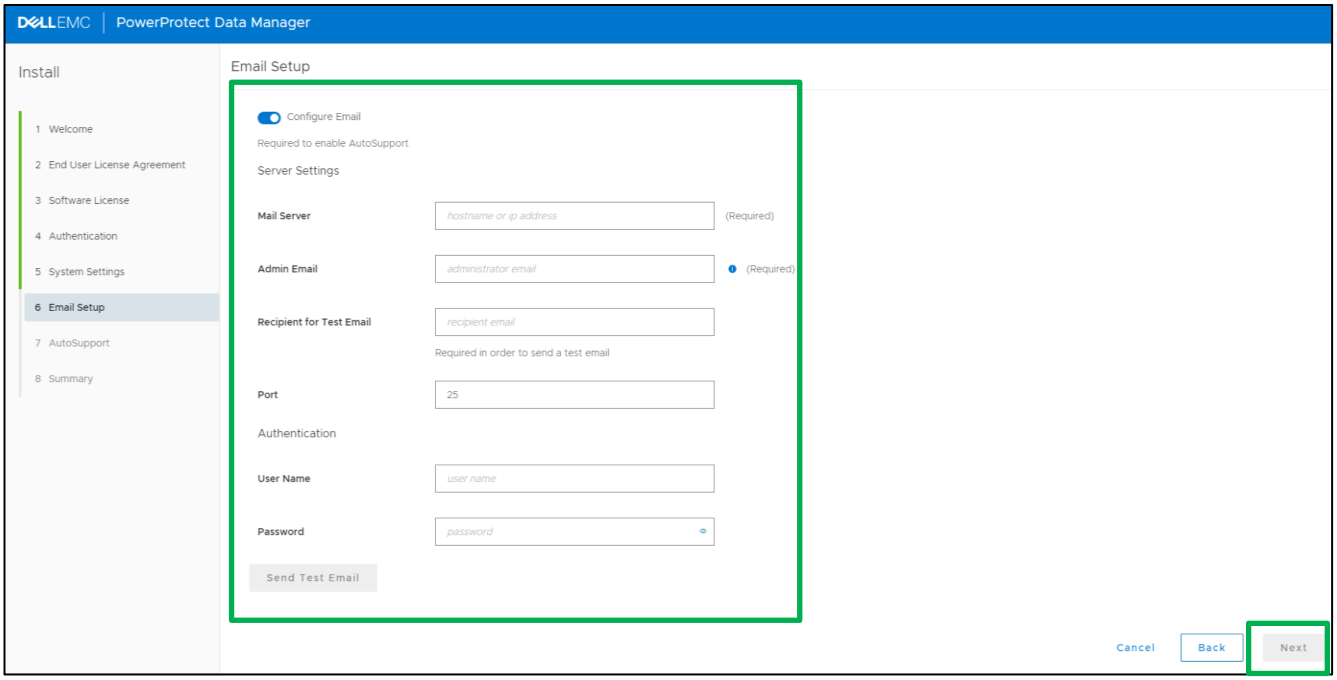
   g. To send a test email to the specified IP address, click **Send Test Email**.

   h. To acknowledge the test email was successfully sent, click **OK**.

   i. To send diagnostic and usage data to Dell EMC 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**.



Email Setup

Configure Email

Required to enable AutoSupport

Server Settings

Mail Server: hostname or ip address (Required)

Admin Email: administrator email (Required)

Recipient for Test Email: recipient email

Required in order to send a test email

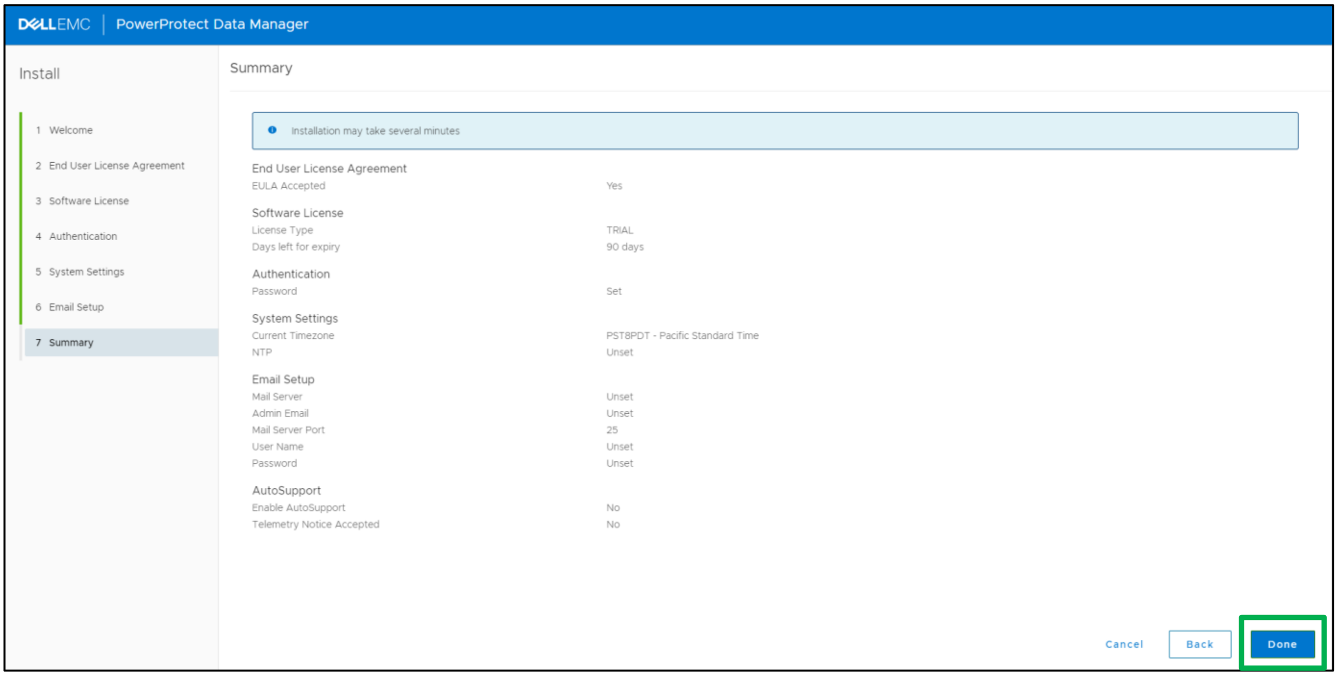
Port: 25

Authentication

User Name: user name

Password: password

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



Summary

Installation may take several minutes

End User License Agreement

EULA Accepted	Yes

Software License

License Type	TRIAL
Days left for expiry	90 days

Authentication

Password	Set

System Settings

Current Timezone	PST8PDT - Pacific Standard Time
NTP	Unset

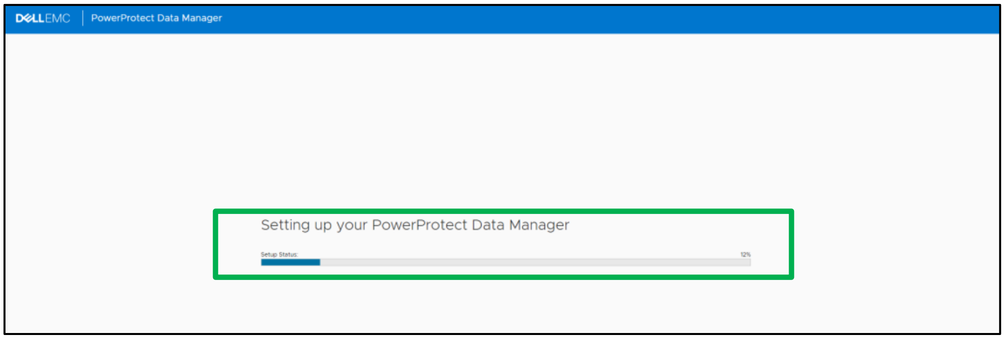
Email Setup

Mail Server	Unset
Admin Email	Unset
Mail Server Port	25
User Name	Unset
Password	Unset

AutoSupport

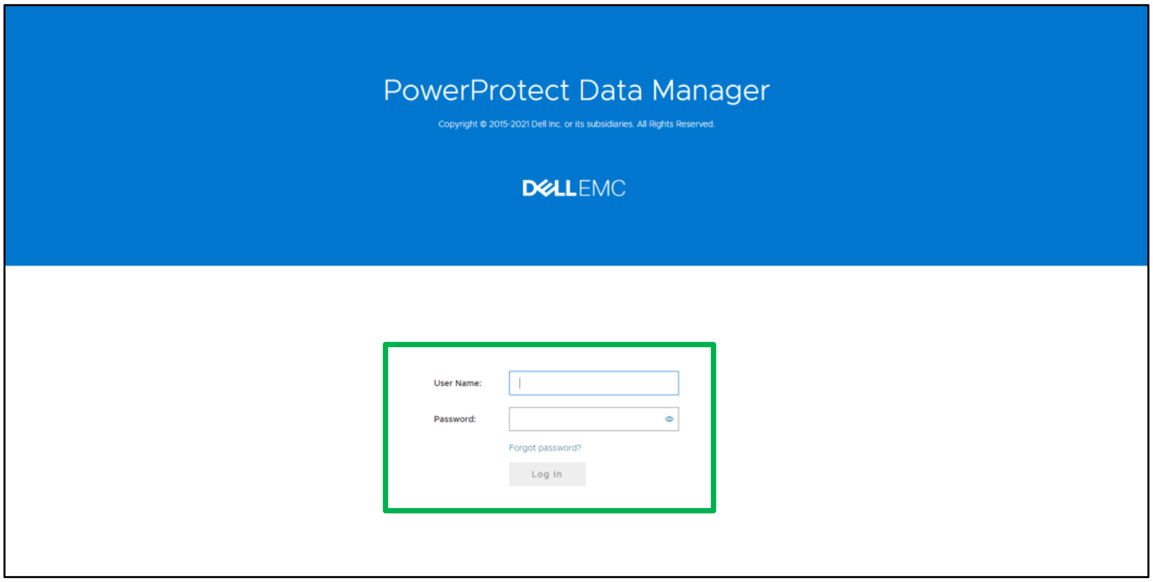
Enable AutoSupport	No
Telemetry Notice Accepted	No

9. Within few minutes Data Manager configuration will be completed and prompt with the login screen.



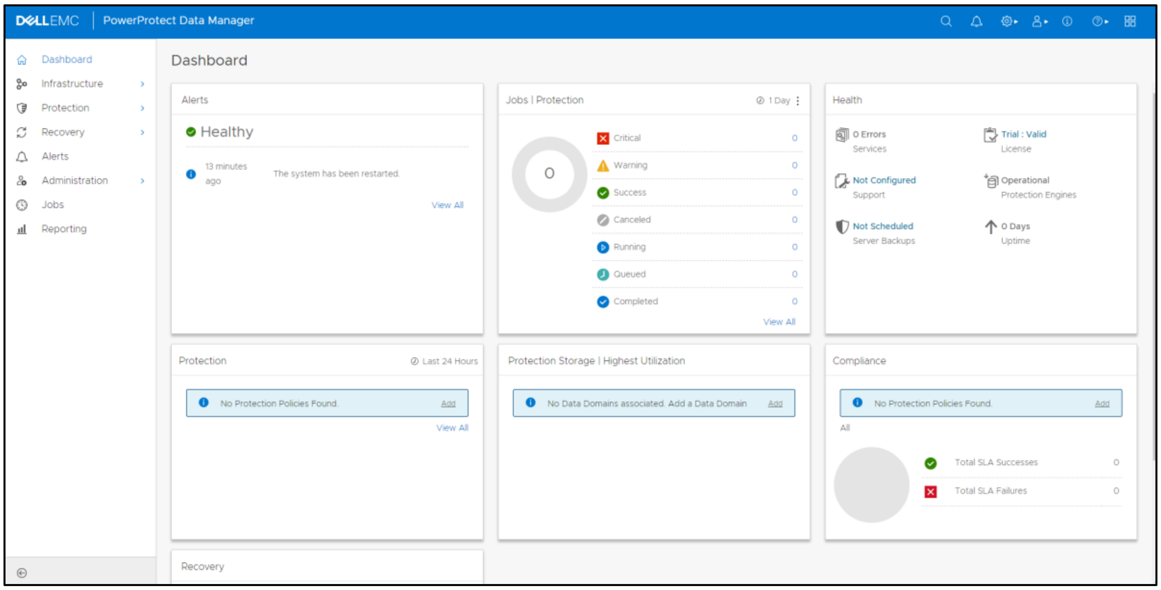
Setting up your PowerProtect Data Manager

10. Login with username as “**admin**” the password set during the configuration.



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

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



The system has been restarted.

No Protection Policies Found.

No Data Domains associated. Add a Data Domain

No Protection Policies Found.

A 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.

A.1 Related resources

Dell EMC PowerProtect Data Manager

- Dell EMC PowerProtect Data Manager Amazon Web Services Deployment Guide
- Dell EMC PowerProtect Data Manager Administration and User Guide
- Dell EMC PowerProtect Data Manager Security Configuration Guide

Dell EMC PowerProtect DD Virtual Edition

- Dell EMC PowerProtect DDVE on Amazon Web Services Installation and Administration Guide
- Dell EMC PowerProtect DD Virtual Edition on Amazon Web Services – Technical White Paper