

PowerProtect DD Virtual Edition on Amazon Web Services

Installation and Administration Guide

DDVE 6.0

Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

Contents

Revision history.....	5
Preface.....	6
Chapter 1: Getting Started.....	7
Purpose of this guide.....	7
Audience.....	7
Prerequisites, limitations, and resources.....	7
Architecture overview.....	8
Chapter 2: Introducing DDVE	10
Introducing DDVE.....	10
DDVE cloud features	10
Chapter 3: Deploying DDVE.....	12
Preparing your environment to deploy DDVE on AWS.....	12
Create an S3 bucket.....	12
Set up role-based access to the AWS object store	14
Deploying DDVE in AWS.....	16
Deploying DDVE using a Cloud Formation Template.....	16
Deploying DDVE manually from the AWS console.....	20
Adding more metadata disks for the DDVE instance.....	23
Expand metadata storage.....	26
Chapter 4: Completing Initial DDVE Configuration.....	27
Configuring DDVE on AWS.....	27
Using the DD System Manager to configure DDVE	27
Using the CLI to configure the DDVE.....	30
Recovering DDVE with system headswap.....	34
Recovering the system.....	36
Chapter 5: Administering DDVE.....	38
Upgrade from M4 to M5 instance type.....	38
Upgrading M5 instance type.....	39
Extensions to DDOS for DDVE.....	39
perf.....	39
System vresource.....	40
DDVE-only commands.....	40
Modified DD OS commands.....	41
Unsupported DD OS commands	42
Troubleshooting performance issues.....	47
Appendix A: Best Practices for Working with DDVE in the Cloud.....	48
ASUP configuration.....	48
AWS licensing.....	48

Storage best practices.....	48
Security best practices.....	50
Appendix B: Networking Best Practices for DDVE in the Cloud.....	53
Network setup in AWS.....	53
Network infrastructure setup.....	54
Appendix C: Installing and Configuring DDVE on Block Storage in the Cloud	56
Overview of DDVE on block storage.....	56
Configuring DDVE on block storage with DD System Manager.....	56

Revision history

Table 1. DDVE 6.0 on AWS Installation and Administration Guide revision history

Revision	Date	Description
01	December 2020	Update for DD OS 7.4

As part of an effort to improve its product lines, we periodically release revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Purpose

This manual describes how to install, configure, and administer DD Virtual Edition (DDVE) systems.

Audience

This manual is intended for use by both system administrators and general users of DD Virtual Edition.

Related documentation

The following publications and websites provide additional information:

- *DD Operating System Release Notes*
- *DD Operating System Initial Configuration Guide*

This manual explains configuration steps that are common to hardware and virtual DD systems.

- *DD Operating System OS Command Reference Guide*

This manual explains how to administer DD systems from the command line.

- *DD Operating System OS Administration Guide*

This manual explains how to administer DD systems with the System Manager graphical user interface.

- *DD Boost for OpenStorage Administration Guide*

This manual explains how to use the DD Boost protocol for data transfer between backup software and DD systems.

- *Avamar, DD and NetWorker Compatibility Guide*: <http://compatibilityguide.emc.com:8080/CompGuideApp/>

This website lists Avamar and NetWorker software support for DDVE.

Where to get help

We support, product, and licensing information can be obtained as follows:

Product information

For documentation, release notes, software updates, or information about products, go to Online Support at <https://support.emc.com>.

Technical support

For technical support of this release of DDVE, go to Online Support at <https://support.emc.com>.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to DPAD.Doc.Feedback@emc.com.

Getting Started

This chapter includes the following topics:

Topics:

- [Purpose of this guide](#)
- [Audience](#)
- [Prerequisites, limitations, and resources](#)
- [Architecture overview](#)

Purpose of this guide

This installation guide is intended as a supplement to the *DD Operating System Administration Guide*, which includes content applicable to all DD systems, including upgrading the DDVE software and using the DD System Manager to monitor DD systems for errors, disk space, and service events.

This guide contains content specific to deploying DD Virtual Edition (DDVE) on Amazon Web Services. Use this guide in conjunction with the *DD Operating System Administration Guide* and applicable AWS documentation.

See [AWS Cloud Formation documentation](#) for more information.

Audience

This document is intended for data protection and storage administrators who want to use Amazon Web Services to back up DD Virtual Edition (DDVE) content. Users should have knowledge of the following technology:

- AWS Management Console
- AWS services, such as AWS IAM, AWS CloudFormation, VPC, AWS security group, and route tables
- Amazon EC2, EBS, and S3 services

Prerequisites, limitations, and resources

Review the general requirements for deploying DDVE on Amazon Web Services (AWS).

Create an AWS account

To deploy DDVE on AWS, you must have an AWS account. To set up an account, go to <https://aws.amazon.com/getting-started/>.

Identity and access management

AWS recommends that you create an IAM user or role for authenticating with AWS and never use root credentials to deploy the CloudFormation template. The IAM user must be allowed to perform AWS CloudFormation actions. The EC2 instance must be granted the IAM role to provide permissions to S3 storage.

The following links provide more information about AWS best practices:

- [Creating-an-IAM-User-in-Your-AWS-Account](#)
- [Using-IAM-Roles](#)
- [What-is-AWS-CloudFormation?](#)

Security and operational best practices

Amazon recommends that you enable AWS CloudTrail logs to enable governance, compliance, and operational and risk auditing of your AWS account. AWS CloudTrail enables you to:

- View the event history of your AWS account activity, including AWS Management Console actions, AWS SDKs, CLI, and other AWS services.
- Identify the initiator of actions, resources involved, and event timing.

This event history helps to simplify security analysis, resource change tracking, and troubleshooting.

The following links provide more information:

- [Working-with-CloudTrail](#)
- [Turn-on-CloudTrail-across-all-regions-and-support-for-Multiple-Trails](#)

AWS service limits and restrictions

The following links provide more information about AWS service limits and restrictions:

- [Bucket-Restrictions-and-Limitations](#)
- [IAM-and-STs-Limits](#)
- [How-do-I-manage-my-AWS-service-limits?](#)
- [AWS-Service-Quotas](#)

Additional links

The following additional links provide more information about the AWS features that are used with a DDVE deployment:

- [Working-with-the-AWS-Management-Console](#)
- [AWS-Cloud-Formation](#)
- [AWS-Identity-and-Access-Management-\(IAM\)](#)
- [Amazon-Virtual-Private-Cloud](#)
- [Amazon-Elastic-Compute-Cloud-Documentation](#)

Architecture overview

DDVE is a virtual deduplication appliance that provides data protection for entry, enterprise, and service provider environments.

The following diagram represents the architecture of the DDVE on AWS solution.

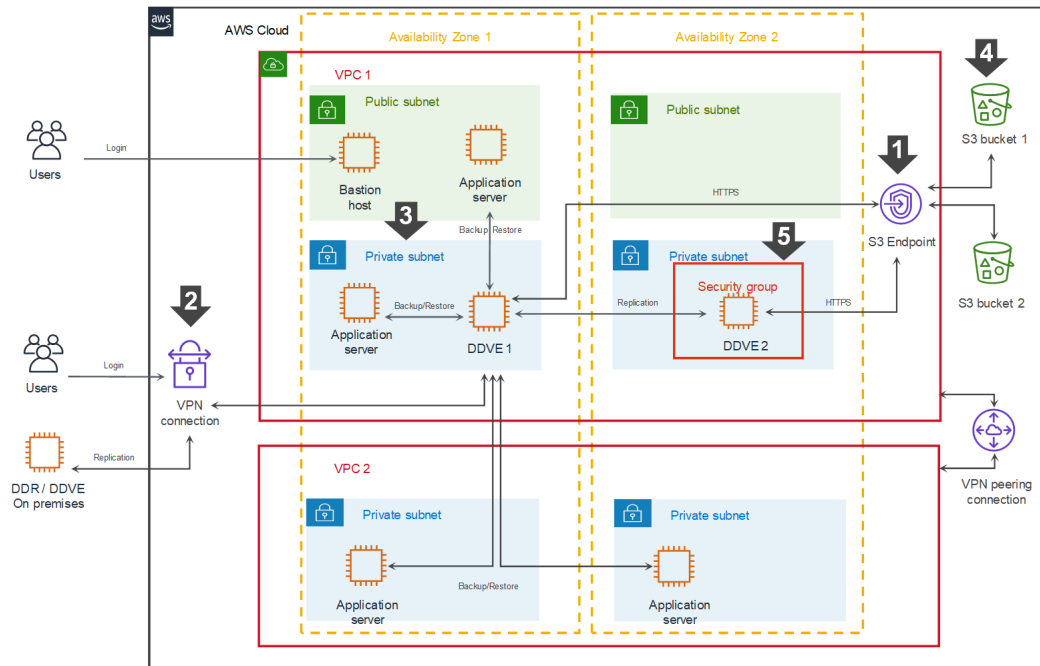


Figure 1. Dell EMC Power Protect DD Virtual Edition (DDVE) on AWS

Legend:

1. To keep data traffic between DDVE and the S3 bucket within the AWS infrastructure, it is recommended that you create an S3 endpoint. The S3 endpoint keeps DDVE from depending on a NAT Gateway or Public IP address to access the S3 bucket.
2. To keep data transfers secure, it is recommended to use a VPN connection to replicate data from an on-premises host to DDVE in the cloud or the opposite way.
3. DDVE is categorized as a backend server. It must be kept in a private subnet with a private address. Never set a public IP address for DDVE.
4. It is recommended that you create the S3 bucket in the region where the DDVE instance is running. A separate bucket per each DDVE is required.
5. All DDVE instances must be secured with the appropriate security group entries.

Typically SSH (Port 22) or HTTPS (Port 443) is used for DDVE inbound access.

HTTPS (443) must be allowed for outbound S3 bucket access for DDVE.

TCP ports 2049 and 2051 are used for DD Boost and replication purposes.

See the DDVE documentation for more information and for a complete list of ports.

Availability Zones

DDVE is deployed within a single Availability Zone (AZ). It can be deployed within additional AZs to provide region redundancy using DD replication capabilities. The solution can also be deployed in alternative regions to provide further redundancy as needed.

Introducing DDVE

This chapter includes the following topics:

Topics:

- [Introducing DDVE](#)
- [DDVE cloud features](#)

Introducing DDVE

DD Virtual Edition (DDVE) is a software-only protection storage appliance: a virtual deduplication appliance that provides data protection for entry, enterprise and service provider environments. Like any DD system, DDVE is always paired with backup software.

DDVE runs the DD Operating System (DD OS), and includes the DD System Manager graphical user interface (GUI) and the DD OS command line interface (CLI) for performing system operations.

DDVE includes the following features:

- High-speed, variable length deduplication for a 10 to 30 times reduction in storage requirements
- Unparalleled data integrity to ensure reliable recovery, and seamless integration with leading backup and archiving applications
- DD Boost to speed backups by 50 percent
- DD Encryption for enhanced security of data
- DD Replicator for network efficient replication that enables faster time-to-DR readiness

DDVE runs on two types of platforms:

- On premises, DDVE supports VMware, Hyper-V, KVM, and VxRail.
- In the cloud, DDVE also runs in the Amazon Web Services (AWS) (cloud and gov cloud), Azure (cloud and gov cloud), VMware Cloud (VMC) on AWS cloud platforms, and Google Cloud Platform (GCP).

For more information about the features and capabilities of DD systems (both physical and virtual), see the *DD Operating System Administration Guide*.

DDVE cloud features

DDVE provides the capabilities of a cloud DD system using the following resource configuration sizes:

Table 2. DDVE on AWS resource configuration size

Type	Resource configuration size
DDVE on Block storage	up to 16 TB
DDVE on S3 storage	up to 256 TB


The following sections list supported DD protocols and features in DDVE.

Supported DD protocols

- DD Boost over IP
- DD Boost FS

Supported DD features

- DD Boost managed file replication (MFR)
- Encryption
- MTree replication
- DD System Manager GUI for DDVE management
- DD Active Tier (DD Cloud Tier is not supported)
- Secure multitenancy (SMT) with Network Isolation Support
- DD Boost/BoostFS for Big Data
- Key Management Interoperability Protocol (KMIP)
- More restricted IPtables settings
- AWS for Government Cloud

 **NOTE:** DDVE supports these replication capabilities:

- Managed file replication and MTree replication
- Replication across availability zones and regions
- Bi-directional replication between on-premises and AWS

The *DD OS Administration Guide*, *DD Boost OST Guide*, *DD Boost for Partner Integration Administration Guide* provide additional information about supported protocols and features.

Deploying DDVE

This chapter includes the following topics:

Topics:

- [Preparing your environment to deploy DDVE on AWS](#)
- [Deploying DDVE in AWS](#)

Preparing your environment to deploy DDVE on AWS

While DDVE is running in AWS cloud, customers can backup and restore their operational data from an S3 object store.

Observe these requirements:

- Storage tier - DDVE on AWS supports Active Tier (Cloud Tier is not supported).
- Storage class - AWS provides multiple storage classes (Standard S3, Standard-IA, and so on). Standard S3 offers high durability, availability, and performance for frequently accessed data. DDVE on AWS supports Standard S3.

The following sections provide general guidelines to deploy, configure, and run DDVE on AWS with Active Tier on S3 storage.

The high-level steps are as follows:

1. Configure the network environment.

For secure access to the DDVE, follow the best practices recommended by AWS for your VPC architecture. Configure the following components:

- VPC
- Subnet
- Route tables
- Security groups
- Network access control list
 - NOTE:** Make sure to allow DDVE inbound and outbound access to S3. If you are unsure which S3 IP addresses to allow, refer to the route table entry for S3 endpoint.
- VPC Gateway endpoint for connectivity to S3
 - NOTE:** DDVE supports standard endpoint format. If you configure firewall rules for endpoints, requests that map to the standard endpoints (*.s3.<region>.amazonaws.com) must be allowed.

[Networking Best Practices for DDVE in the Cloud](#) on page 53 provides more information.

2. Create an S3 bucket.
3. Configure role-based access to the AWS object store.
4. For secure login to DDVE, create an EC2 key access pair. See [Amazon EC2 Key Pairs](#) for instructions.

Create an S3 bucket

About this task

Create a bucket in S3 and make note of the bucket name. The bucket name is used in the IAM policy template to get access to the bucket. It is also used to create the object store profile on the DDVE.

Steps

1. Log in to the AWS console. Select **Services** > **S3**.
2. Click **Create bucket** and enter the bucket name and region.

NOTE: Observe these requirements when creating a bucket for DDVE use:

- To access an S3 bucket, AWS recommends using hosted-style URLs (where domain name includes the bucket name) instead of path-style URLs. For hosted-style URLs to work, do not use dots (".") in the bucket name.
- Create the bucket in the same region as the DDVE instance.
- Provide a bucket name that is no longer than 48 characters.
- Do not enable bucket versioning for the bucket that is associated with the DDVE for these reasons:
 - Versioning adds to storage costs because older versions of the objects are retained despite running the DDVE garbage collection process.
 - Enabling versioning can also cause potential performance issues.

3. Click **Create Bucket**.

The screenshot shows the AWS Management Console 'Create bucket' page. The 'General configuration' section has 'Bucket name' set to 'ddve-bucket' and 'Region' set to 'US East (N. Virginia) us-east-1'. The 'Bucket settings for Block Public Access' section has 'Block all public access' checked. Below this, four sub-settings are also checked: 'Block public access to buckets and objects granted through new access control lists (ACLs)', 'Block public access to buckets and objects granted through any access control lists (ACLs)', 'Block public access to buckets and objects granted through new public bucket or access point policies', and 'Block public and cross-account access to buckets and objects through any public bucket or access point policies'. At the bottom, there are 'Cancel' and 'Create bucket' buttons.

NOTE: Do not set up life-cycle rules for this bucket. Life-cycle rules could cause loss of critical data from the object store.

Set up role-based access to the AWS object store

Object store in AWS uses role-based access for S3 access. To access the S3 bucket, create and attach the Identity and Access Management (IAM) role to DDVE.

Prerequisites

To create the IAM role and the policy that is associated with the role, the AWS user must have the necessary IAM privileges. The following IAM privileges and actions are required to create and attach the IAM role:

```
"iam:AddRoleToInstanceProfile",
    "iam:AttachRolePolicy",
    "iam:CreateRole",
    "iam>DeleteRole",
    "iam>DeleteRolePolicy",
    "iam:DetachRolePolicy",
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:ListRolePolicies",
    "iam:ListRoles",
    "iam:PassRole",
    "iam:RemoveRoleFromInstanceProfile",
    "iam:UpdateRolePolicy",
    "iam:CreateInstanceProfile",
    "iam:PutRolePolicy",
    "iam>DeleteInstanceProfile"
```

About this task

When the role is attached to DDVE, the S3 object store credentials are automatically fetched. The AWS infrastructure periodically rotates the access credentials. The DDVE automatically fetches the new credentials before the old credentials expire.

Steps

1. Create the policy to attach with the IAM role:
 - a. Sign in to the AWS Management Console and open the IAM Service Console.
 - b. In the navigation pane of the IAM console, select **Policies** > **Create policy**.
 - c. Do one of the following:

- Create a policy for AWS Standard Cloud:

In the **Create policy** web page, select the **JSON** tab. Replace the text under the JSON tab with the following content. Replace `my-bucket-name` with the name of the bucket that was created previously.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::my-bucket-name",
        "arn:aws:s3:::my-bucket-name/*"
      ]
    }
  ]
}
```

- Create a policy for AWS Gov Cloud:

In the **Create policy** web page, select the **JSON** tab. Replace the text under the JSON tab with the following content. Replace `my-bucket-name` with the name of the bucket that was created previously. For the resource tag below, use `arn:aws-us-gov:s3:::my-bucket-name` for AWS Gov clouds.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws-us-gov:s3::my-bucket-name",
        "arn:aws-us-gov:s3::my-bucket-name/*"
      ]
    }
  ]
}
```

- d. Verify this information, and then click **Review policy**.
- e. Provide a name and description for the policy, and click **Create policy**.

Create policy 1 2

Review policy

Name ddve-s3-access-policy
Use alphanumeric and "+,=,@" characters. Maximum 128 characters.

Description This policy defines the actions permitted by the DDVE instance on the given resource, i.e. s3 bucket in this context
Maximum 1000 characters. Use alphanumeric and "+,=,@" characters.

Summary

Service	Access level	Resource	Request condition
Allow (1 of 235 services) Show remaining 234			
S3	Limited: List, Read, Write	Multiple	None

* Required Cancel Previous **Create policy**

NOTE: Make a note of the policy name. It will be used to attach the policy to the role in the next step.

2. Create the role for S3 bucket access:
 - a. In the navigation pane of the IAM console, select **Roles** > **Create role**.
 - b. On the **Create role** page:
 - i. For **Select type of trusted entity**, select **AWS service**.
 - ii. For **Choose the service that will use this role**, select **EC2**, and then click **Next Permissions**.
 - c. On the **Attach permissions policies** page, select the policy that you created in the previous step. Select **Next Tags** to create a tag for the role.

Create role

1 2 3 4

▼ Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy

Filter policies ddve-s3-access-policy Showing 1 result

	Policy name	Used as
<input checked="" type="checkbox"/>	ddve-s3-access-policy	Permissions policy (2)

► Set permissions boundary

* Required Cancel Previous Next: Tags

Figure 2. Creating a role

- d. Click **Next:Review**. In the **Review** section, provide a name for the role and click **Create role**.

Next steps

You must attach the role to the DDVE instance before it can be configured. This task can be done during or after deployment.

Deploying DDVE in AWS

You can deploy DDVE on AWS in two ways.

About this task

Methods of deployment in AWS:

- Cloud Formation Template (CFT) from AWS marketplace
- DDVE Manual Deployment from AWS console

Dell EMC strongly recommends using the CFT method because it automatically creates and attaches NV RAM and metadata disks in the correct order according to [Storage best practices](#).

Deploying DDVE using a Cloud Formation Template

This method is recommended.

Steps

1. Go to the appropriate Website:
 - For deployment in AWS standard cloud, use <https://aws.amazon.com/marketplace>.
 - For deployment in AWS Gov cloud, use <https://aws.amazon.com/mp/govcloud/>.
2. Search for **PowerProtect DD Virtual**.
3. Select **Dell EMC PowerProtect DD Virtual Edition (DDVE) <version_number>** and click **Continue to Subscribe**.

NOTE: Your screen might be different than shown in the following figure.

Dell EMC PowerProtect DD Virtual Edition (DDVE)

By: [Dell EMC](#) Latest Version: PowerProtect DD VE v4.0 with 7.0.0.5

Dell EMC PowerProtect DD Virtual Edition (DDVE) is a software-defined version of Dell EMC Data Domain, the world's most trusted protection storage. It can be downloaded, deployed and

[Show more](#)

Linux/Unix ☆☆☆☆ 0 AWS reviews [BYOL](#)

[Continue to Subscribe](#)

[Save to List](#)

Typical Total Price
\$0.800/hr

Total pricing per instance for services hosted on m4.4xlarge in US East (N. Virginia). [View Details](#)

Overview Pricing Usage Support Reviews

Product Overview

Dell EMC PowerProtect DD Virtual Edition (DDVE) is the software-defined data protection solution based on industry-leading Dell EMC Data Domain, the world's most trusted protection storage. DDVE can now deliver increased transactional and operational efficiencies, reliability and lower TCO by utilizing object storage (standard S3). DDVE can now run up to 96TB instances. With the latest release of DD OS 6.2, DDVE extends support to AWS DevCloud.

Version	PowerProtect DD VE v4.0 with 7.0.0.5 Show other versions
By	Dell EMC
Video	See Product Video
Categories	Storage & Backup

Highlights

- DDVE can now run in up to 96TB instances - a boost up from 16TB in the previous releases! Now supports AWS GovCloud!
- Achieve increased transactional and operational efficiencies, reliability and lower TCO by utilizing object storage in addition to block storage.
- 0.5 TB Embedded Trial license, Up to 96TB capacity paid version, Data store in S3 standard

Figure 3. Deploying DDVE using a CFT

4. Click **Continue to Configuration**.

Dell EMC PowerProtect DD Virtual Edition (DDVE)

[Continue to Configuration](#)

[< Product Detail](#) [Subscribe](#)

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 agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement (EULA). Your use of AWS services is subject to the [AWS Customer Agreement](#).

Product	Effective date	Expiration date	Action
Dell EMC PowerProtect DD Virtual Edition (DDVE)	1/17/2019	N/A	Show Details

Figure 4. Subscribing to the software

5. Select the following configuration, and then click **Continue to Launch**.

- **Fulfillment Option**—Select **Cloud Formation Template**.
- **Software Version**—Select the correct version.
- **Region**—Select where the DDVE is to deploy.

Dell EMC Dell EMC PowerProtect DD Virtual Edition (DDVE) Continue to Launch

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.

Fulfillment Option

CloudFormation Template CloudFormation Template: Deploy a complete solution configuration using a CloudFormation template

DD VE Deployment - CloudFormation (Recommended)

Software Version

PowerProtect DD VE v4.0 with 7 Whats in This Version: Dell EMC PowerProtect DD Virtual Edition (DDVE) running on m4.xlarge. [Learn more](#)

Region

US East (N. Virginia)

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 DD Virtual Edition (DDVE) \$0/hr

BYOL running on m4.xlarge

Figure 5. Configuring software

- Review the configuration details, select **Launch the Cloud Formation template**, and then select **Launch**. The template URL is populated.
- Click **Next**.

aws Services Resource Groups

CloudFormation > Stacks > Create stack

Create stack

Prerequisite - Prepare template

Prepare template

☒ 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

☒ Amazon S3 URL ☐ Upload a template file

Amazon S3 URL

<https://s3.amazonaws.com/awssmp-fulfillment-cf-templates-prod/3cc6672f-1de3-47d6-8eb2-31f9ebd815c7.3a8e49d9-7d34-4332-9038-5c91aa2b1.template>

Amazon S3 template URL

S3 URL: <https://s3.amazonaws.com/awssmp-fulfillment-cf-templates-prod/3cc6672f-1de3-47d6-8eb2-31f9ebd815c7.3a8e49d9-7d34-4332-9038-5c91aa2b1.template> View in Designer

Cancel Next

- Enter the following values to create the stack.

- Stack name
- DDVE Model—Four options are available:
 - 16 TB-Model—m5.xlarge
 - 32 TB-Model—m5.2xlarge
 - 96 TB-Model—m5.4xlarge
 - 256 TB-Model—m5.8xlarge

System capacity	Instance type	vCPU	Memory (GiB)	Number of default metadata disks
16 TB	M5.xlarge	4	16	2 x 1 TiB
32 TB	M5.2xlarge	8	32	4 x 1 TiB
96 TB	M5.4xlarge	16	64	10 x 1 TiB
256 TB	M5.8xlarge	32	128	13 x 2 TiB

- Override default metadata disks— You can choose to override the default number of metadata disks by selecting a value from 1-24. The maximum number of metadata disks that can be attached to a DDVE instance in AWS is 24.

NOTE: Only the number of metadata disks can be overridden. The size of individual disks cannot be changed.

- DDVE name tag
- IAM Role for S3 access—Type in the correct IAM role to be attached to the DDVE.
- Key pair—Select an existing key pair from the drop-down list.
- Subnet ID
- Security Groups

The screenshot shows the 'Specify stack details' page in the AWS CloudFormation console. The stack name is 'ddve-stack-test'. Under 'Parameters', the 'DDVE Instance Configuration' section shows 'DDVE Model' set to '16TB-Model--m5.xlarge'. The 'Override default Metadata disks' section is set to 'Default'. The 'DDVE Name Tag' is 'ddve-test'. The 'IAM Role for S3 access' is 'ddve-test-role'. The 'Key Pair' is 'ddve-bastion'. The 'DDVE Network' section shows 'Subnet ID' as 'subnet-0765540ca56d3b51d (10.3.1.0/24) (ddve-infra-private-subnet)' and 'Security Groups' as 'ddve-private-subnet-sg (sg-0da4068762ad9d8ce) (ddve-infra-private-sg)'. Navigation buttons at the bottom include 'Cancel', 'Previous', and 'Next'.

NOTE: The values in this figure are examples only. Replace them with values from your setup.

9. Continue stack configuration as needed. Click **Next**.
10. Review the stack configuration and click **Create Stack**.
11. Check the status of the stack you create on the **ddve-stack-test** page.

The screenshot shows the 'ddve-stack-test' stack page in the AWS CloudFormation console. The stack is in the 'CREATE_COMPLETE' status. The 'Overview' section displays the following details:

Stack ID	awscloudformation-us-east-1:385125126520stack/ddve-stack-test/2af8330d-c260-11e9-ba87-b0d71499a99	Description	AWS CloudFormation for DD VE: This template creates one DD VE Instance attached with Meta Data Disks. WARNING! This template creates an Amazon EC2 instance and EBS Volumes. You will be billed for the AWS resources used if you create a stack from this template.
Status	CREATE_COMPLETE	Status reason	-
Root stack	-	Parent stack	-
Created time	2019-09-08 10:43:29 UTC-0700	Deleted time	-
Updated time	-		
Drift status	NOT_CHECKED	Last drift check time	-
Termination protection	Disabled	IAM role	-

12. When the stack creation is complete, go to the EC2 instances and select the region to deploy the DDVE. Use the DDVE name tag from step 8 and verify that the corresponding EC2 instance is running.

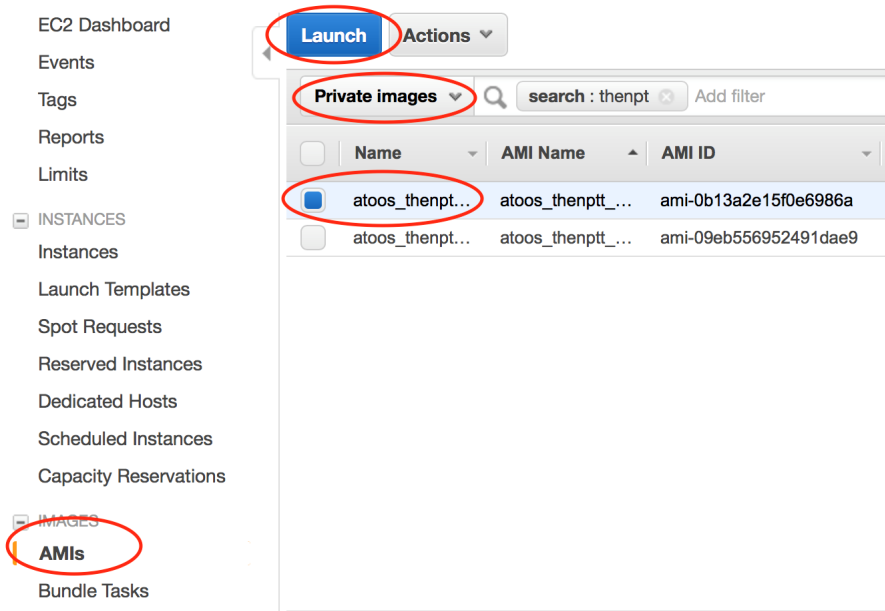
NOTE: Avoid disabling or modifying the primary interface settings. The primary interface in cloud deployments has the default gateway setting and is the only interface with which the DDVE can connect to the metadata server. The metadata server is critical for DDVE operation.

Deploying DDVE manually from the AWS console

This is an alternate approach for deployment.

Steps

- 1. Login to AWS console and navigate to the EC2 instances link.
- 2. Under the **EC2 instances** tab, select **Private Images**. Select the AMI image from the region in which you wish to deploy DDVE, and then click **Launch**.



- 3. Select the instance type from the three supported instance types. Click **Configure Instance Details**. For more details, refer to [Storage best practices](#).

1. Choose AMI2. Choose Instance Type3. Configure Instance4. Add Storage5. Add Tags6. Configure Security Group7. Review

Step 2: Choose an Instance Type

<input type="checkbox"/>	General purpose	m5.large	2	8	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5.xlarge	4	16	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5.2xlarge	8	32	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5.4xlarge	16	64	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5.8xlarge	32	128	EBS only	Yes	10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5.12xlarge	48	192	EBS only	Yes	10 Gigabit	Yes

- 4. Select the VPC and subnet in which to deploy DDVE, and select the IAM role that you created in the previous section. Selecting the role during deployment automatically attaches it to this DDVE instance. If you did not previously create the VPC, subnet, or the IAM role, you can create them in this step. When you are done, click **Add Storage**.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of lower prices, or request Dedicated Hosts to run on dedicated hardware.

Number of instances [Launch into Auto Scaling Group](#)

Purchasing option ☐ Request Spot instances

Network [Create new VPC](#)

Subnet [Create new subnet](#)
236 IP Addresses available

Auto-assign Public IP ☐ Use subnet setting (Disable)

Placement group ☐ Add instance to placement group

Capacity Reservation [Create new Capacity Reservation](#)

IAM role [Create new IAM role](#)

CPU options ☐ Specify CPU options

Shutdown behavior

5. Add the NVRAM disk and metadata disks as shown below. Then click **Add Tags**.
 - a. Add a 10 GiB NVRAM disk (highlighted in red).
 - b. Add the metadata disks (highlighted in green) according to the following configuration table.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/sda1	snap-00a675505a78b83ca	250	General Purpose SSD (gp2)	750 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted
EBS	/dev/sdb	Search (case-insensitive)	10	General Purpose SSD (gp2)	100 / 3000	N/A	<input type="checkbox"/>	Not Encrypted
EBS	/dev/sdc	Search (case-insensitive)	1024	General Purpose SSD (gp2)	3072	N/A	<input type="checkbox"/>	Not Encrypted

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Tags](#)

NOTE: It is important to add the NVRAM disk **before** adding the metadata disks. Adding them in a different order causes an unsupported hardware configuration error. Also, ensure that the EBS volume type is GP2 for all disks.

Table 3. Recommended configuration

Instance Type	Number of metadata disks	Size of each metadata disk	Object store capacity
M5.xlarge	2	1 TiB	16 TB
M5.2xlarge	4	1 TiB	32 TB
M5.4xlarge	10	1 TiB	96 TB
M5.8xlarge	13	2 TiB	256 TB

NOTE: By default, the recommended metadata storage is 10% of the total capacity. This recommendation is based on a 10x deduplication ratio and a 2x compression ratio. For workloads with higher deduplication ratios, you can add more metadata disks.

6. Add the tags as shown in the following figure, and then click **Configure Security Groups**.

Adding tags enables you to easily search for volumes and instances.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)	Instances	Volumes
Name	ddve-test	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Add another tag](#) (Up to 50 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

7. Select from an existing security group. If you haven't created one previously, you can create it now. Click **Review and Launch**.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules that allow unrestricted access to the HTTP and HTTPS ports to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports to reach your instance.

Assign a security group: ☐ Create a new security group ☒ Select an existing security group

8. Review the configuration details, and then click **Launch**.
9. Select a key pair value or create a new key pair value for this instance, and then click **Launch Instance**.

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. [Learn more about removing existing key pairs from a public AMI.](#)

Choose an existing key pair

Select a key pair

demo-key

☒ I acknowledge that I have access to the selected private key file (demo-key.pem), and that without this file, I won't be able to log into my instance.

[Cancel](#) [Launch Instances](#)

Select an existing key pair or create a new key pair



A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair

Key pair name

ddve-test-key

Download Key Pair

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel

Launch Instances

10. Click **View instances** to navigate to the EC2 instance tab. Search for the tag you created in step 6.

Launch Status

The following instance launches have been initiated: i-0feff568addddaad8 View launch log

Get notified of estimated charges
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click **View instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. [Find out](#) how to connect to your instances.

Here are some helpful resources to get you started

- How to connect to your Linux instance
- Learn about AWS Free Usage Tier
- Amazon EC2: User Guide
- Amazon EC2: Discussion Forum

While your instances are launching you can also

- Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)
- Create and attach additional EBS volumes (Additional charges may apply)
- Manage security groups

View Instances

EC2 Dashboard

Launch Instance Connect Actions

search: ddve-test Add filter

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
ddve-test	i-0001697ae69254e6...	m4.xlarge	us-east-1a	running	initializing	None	

NOTE: Avoid disabling or modifying the primary interface settings. The primary interface in cloud deployments has the default gateway setting and is the only interface with which the DDVE can connect to the metadata server. The metadata server is critical for DDVE operation.

Adding more metadata disks for the DDVE instance

If required, more metadata disks can be added to the DDVE instance from the AWS console.

Prerequisites

AWS DDVE instances support adding only up to 24 metadata disks. If you reach the limit for adding metadata disks, you can choose to expand the existing metadata disks. See [Expand metadata storage](#) on page 26 for details.

Steps

1. Log in to the AWS console.

2. Select **EC2** dashboard under services. Navigate to the **Elastic Block Store** pane and click **Volumes**.
3. Provide the following details. Then click **Create Volume**.
 - **Volume Type**: Select GP2.
 - **Size (GiB)**: Select 1024 for 16/32/96 TB DDVE instance and 2048 for 256 TB DDVE instance.
 - **Availability Zone (AZ)**: Choose the same AZ in which the DDVE instance is deployed.
 - **Name Tag**: Add a name tag for the volume to filter it in searches.

Leave **Snapshot ID** blank.

The screenshot shows the AWS 'Create Volume' page. The configuration is as follows:

- Volume Type**: General Purpose SSD (gp2)
- Size (GiB)**: 1024 (Min: 1 GiB, Max: 16384 GiB)
- IOPS**: 3072 (Baseline of 3 IOPS per GiB)
- Availability Zone***: us-east-1a
- Throughput (MB/s)**: Not applicable
- Snapshot ID**: Select a snapshot
- Encryption**: ☐ Encrypt this volume
- Tags**:

Key	Value
Name	ddve-volume

At the bottom, there is a 'Cancel' button and a 'Create Volume' button.

4. In the **Volumes** tab, enter the name tag (created in previous step) for the volume. Select the volume, click **Actions**, and select **Attach Volume**.

Create Volume

Actions

Add filter

<input type="checkbox"/>	Name	Volume ID	Size	Volume Type	IOPS
<input type="checkbox"/>	ddve-volume	vol-0c75905eb3fcae350	1024 GiB	gp2	3072

Volumes: **vol-0c75905eb3fcae350 (ddve-volume)**

Description

Status Checks



Monitoring


Tags

Volume ID	vol-0c75905eb3fcae350
Alarm status	None
Snapshot	-
Availability Zone	us-east-1a
Encryption	Not Encrypted
KMS Key ID	
KMS Key Aliases	
KMS Key ARN	
Multi-Attach Enabled	No

5. In the attach volume window, enter the instance ID and device name:
- Instance:** Enter the name/instance ID of the DDVE instance, and select the correct instance from the list of instance options.
 - Device:** Based on the instance, a default device name is automatically populated in this field. The device names for existing volumes on this instance can be `/dev/sd*` or `/dev/xvd*`. Ensure that the new volume being attached follows the device naming convention for other metadata disks on this instance.

Attach Volume

Volume		vol-0c75905eb3fcae350 (ddve-volume) in us-east-1a
Instance		<div>i-0215da5c490927f76</div> in us-east-1a
Device		<div>/dev/sdf</div> <div>Linux Devices: /dev/sdf through /dev/sdp</div>


NOTE: You can check the device names for an instance by selecting an instance in the EC2 dashboard and viewing the block device names for its EBS volumes:

Root device type	ebs
Root device	/dev/sda1
Block devices	/dev/sda1
	/dev/sdb
	/dev/sdc
	/dev/sdd
Elastic Graphics ID	-
Elastic Inference accelerator ID	-


6. To create and attach additional metadata disks to the DDVE instance, repeat steps 2 on page 24 to 5 on page 25.
7. To configure the metadata storage using CLI or DDSM, log in to the DDVE instance.

Using CLI:

- Run the `disk show hardware` command to verify that the new metadata disk or disks are successfully added to the DDVE instance.
- Run the `storage add dev<n>` command to add the new metadata disk or disks to the active tier.
- Run the `filesystem expand` to make the newly added metadata disk or disks available to the filesystem.

Using DDSM:

Alternatively, you can configure the storage using DDSM. Click **Hardware > Storage > Configure Storage**.

 **NOTE:** Do not manually configure spindle groups. Spindle group configuration occurs automatically.

Expand metadata storage

Expand metadata storage by increasing the size of existing metadata disks.


Prerequisites

It is recommended that you expand metadata storage by adding new metadata disks. When the total number of metadata disks reaches its limit, you can expand metadata storage by increasing the size of existing metadata disks.

- Before expanding metadata storage, disable the file system.
- You cannot expand the first metadata disk.
- When expanding the size of an existing metadata disk, it is recommended to expand it in 1 TiB increments.
- Shrinking the metadata disk is not supported.

Steps

1. Shut down the DDVE instance by using the system `system poweroff` command from the CLI.
2. Log in to the AWS web console.
 - a. From the **Volumes** tab, select the metadata disk that you want to expand.

 **NOTE:** The first metadata disk is not available for expansion.

- b. Click **Actions > Modify Volume**.
 - c. Change the size of the metadata disk (for example, from 1024 TiB to 2048 TiB), and click **Modify**.
3. To increase the size of other metadata disks, if required, repeat step 2 on page 26.
 4. From the AWS web console, select the DDVE and start it.
 5. Disable the file system with the `filesystem disable` command.
 6. Expand metadata storage with the `filesystem expand` command.
 7. Enable the file system by using the `filesystem enable` command.
 8. To confirm the metadata storage expansion, use the `filesystem show space tier active local-metadata` command.

Completing Initial DDVE Configuration

This chapter includes the following topics:

Topics:

- [Configuring DDVE on AWS](#)
- [Recovering DDVE with system headswap](#)
- [Recovering the system](#)

Configuring DDVE on AWS

You can use the DDSM interface or the CLI to configure the DDVE on AWS.

Prerequisites

Ensure that you complete the following:

- Consider metadata storage size and count requirements. See [Storage Best Practices](#).
- Create an S3 bucket in the same region in which DDVE is deployed. [Create a bucket in AWS](#) provides instructions.
- Make a note of the bucket name. You will need it to create the object store profile.

About this task

Use one of the following procedures to configure the DDVE on AWS:


- [Using the DD System Manager to configure DDVE](#) on page 27
- [Using the CLI to configure the DDVE](#) on page 30

Using the DD System Manager to configure DDVE

Use this procedure to configure DDVE on AWS using the DD System Manager interface.

Steps

1. Log in to DD System Manager using the DDVE IP address. The default login credentials for the DDVE instance are:
 - Username: sysadmin
 - AWS default password: Default sysadmin password is the EC2 instance-id for the DDVE
2. Add licenses. Select from the list of options of licenses to apply:
 - Pre-Installed Evaluation License (provides 45 days of limited access to DDVE software for evaluation purposes and may only be used in a non-production environment.)

 **NOTE:** If you begin the configuration with the evaluation license, but want to purchase a license later, you need the Node Locking ID for the DDVE instance. Click **Administration > Licenses** to view the Node Locking ID.

 - License File
 - License Server (if available)
3. Accept the End User License Agreement.
4. The configuration wizard is launched automatically. Leave the Network settings as default and click **No** to proceed.
5. Click **Yes** to set up File System configuration.
6. For the **Storage Type**, select **Object Store** and enter the passphrase and the bucket name. For AWS GovCloud, there is an option to select the FIPS endpoint, as shown in the following figure.

7. For Configure CA Certificates, import the Baltimore CyberTrust Root certificate to communicate with AWS S3 Object Store.
8. Configure Storage. Under **Available Storage**, select the disks and click **Add to Metadata** to move them to the Metadata Storage section. Add the disks to the active tier to add the metadata storage disk to the instance.

9. On the **File System Summary Page**, select the **Summary** tab to review all the fields. Select **Enable file system after creation** and click **Submit**.
10. The file system is created and enabled.

11. Click **OK** to go to the **System Settings** tab.
12. Change the DDVE password.

13. Configure the email server as required.

14. Click **Submit** to save the system settings. Close the wizard.

15. DDVE must have accurate and consistent time synchronization for object store communication. DDVE can synchronize time by using Amazon Time Sync Service or by configuring an NTP server.

Option	Description
Method 1 - Using Amazon Time Sync Service (recommended)	By default, DDVE uses Amazon Time Sync Service for time synchronization through a chrony client. DDVE does not require Internet access or configuration of security group rules to use this time synchronization service. Dell EMC recommends using the Amazon Time Sync Service.
Method 2 - Configuring NTP server (not recommended)	<p>To override the default, you can configure an NTP server on the DDVE:</p> <ol style="list-style-type: none"> Select Administration > Settings. Select More Tasks > Configure Time Settings. Under More Tasks, select NTP > Manually Configure and add the NTP servers as <code>0.amazon.pool.ntp.org</code>. <p>NOTE: To switch to the default service (Amazon Time Sync), select Administration > Settings > More Tasks > Configure Time Settings > Choose None.</p>

Results

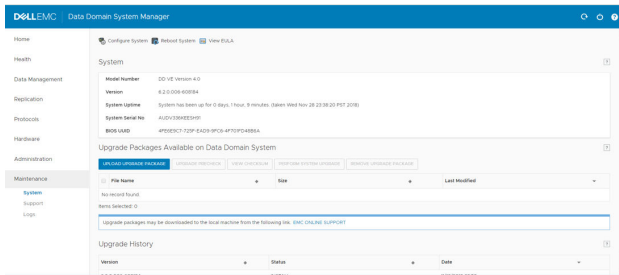
The DDVE configuration is complete.

Updating the configuration

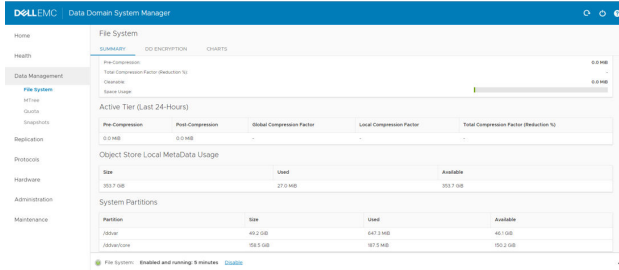
If you modify the object-store profile or make other changes after the initial DDVE configuration, you will need to relaunch the configuration wizard.

Steps

1. Select **Maintenance > System**.
2. Select **Configuration System**.



3. Select **Data Management > File System** to view object store local metadata storage.



Using the CLI to configure the DDVE

You can log in through SSH to configure the DDVE using the command line interface (CLI). Authentication using EC2 key access pair and username and password are supported.

Steps

1. Log in to the DDVE instance to configure the system. The default login credentials for the DDVE instance are:

- Username: sysadmin
- AWS default password: Default sysadmin password is the EC2 instance-id for the DDVE.

```
# ssh sysadmin@<IP address of DDVE>
EMC DD Virtual Edition
Password:

Welcome to Data Domain OS 7.2.0.5-xyz
sysadmin@myddve0#
```

2. During the first login, users are prompted to accept the EULA and change the password.
3. The configuration wizard launches.
4. Follow the steps in the wizard to add an elicense and to configure object store.

NOTE:

- If an elicense file cannot be found in `/ddr/var`, the license can be pasted directly in the wizard.
- The System Passphrase is required to encrypt the object store credentials. If file system encryption is enabled, the System Passphrase is also used to encrypt keys.
- For AWS, the profile creation requires that you import the Baltimore CyberTrust Root certificate to communicate with the object store.
- For AWS GovCloud, profile creation has an additional option to enable the FIPS endpoint.

```
Welcome to Data Domain OS *.*.*-*****
-----
Press any key then hit enter to acknowledge the receipt of EULA information: q
Enter new password:
Re-enter new password:
Passwords matched.

Security Officer
Do you want to create security officer ? (yes|no) [no]:
```

```

    Do you want to configure system using GUI wizard (yes|no) [no]:

Network Configuration
    Configure Network at this time (yes|no) [no]:

eLicenses Configuration
    Configure eLicenses at this time (yes|no) [no]: yes

Available eLicense Files
    # File Name
    - -----
    1 elicense.lic
    - -----

    Do you want to use an existing eLicense file (yes|no)[yes]: yes
    Enter the index of eLicense file [1|cancel]: 1

Pending eLicense Settings
Existing Licenses:

.....

New Licenses:
    Capacity licenses:
    ## Feature Capacity Type State Expiration Date Note
    -- -----
    1 CAPACITY 87.31 TiB permanent (int) active n/a
    -- -----

** New license(s) will overwrite existing license(s).
    Do you want to save these settings (Save|Cancel|Retry): Save

Successfully updated eLicenses.

Filesystem Configuration
    Configure Filesystem at this time (yes|no) [no]: no

System Configuration
    Configure System at this time (yes|no) [no]: no

CIFS Configuration
    Configure CIFS at this time (yes|no) [no]: no

NFS Configuration
    Configure NFS at this time (yes|no) [no]: no

SMT Configuration
    Configure SMT at this time (yes|no) [no]: no

Storage object-store profile Configuration
    Configure Storage object-store profile at this time (yes|no) [no]: yes

    Do you want to enable object store (yes|no)[yes]: yes

A passphrase needs to be set on the system.
Enter new passphrase:
Re-enter new passphrase:
Passphrases matched.
DD VE is running in AWS. Role-based access will be used to access s3.
    Enter the bucket name: simp-test-bucket

    Object-store endpoint needs the Baltimore CyberTrust Root certificate to be
imported.
    Do you want to import that certificate with below fingerprint?
    D4:DE:20:D0:5E:66:FC:53:FE:1A:50:88:2C:78:DB:28:52:CA:E4:74 (yes|no) [yes]: yes

Pending Object Store Settings
    Bucket name: simp-test-bucket

    Do you want to save these settings (Save|Cancel|Retry): Save
The passphrase is set

```

```
Successfully set object store profile.  
Configuration complete.
```

5. Run the following command to view the disks that are attached to the DDVE:

```
# disk show hardware  
Disk      Slot      Manufacturer/Model      Firmware      Serial No.      Capacity      Type  
-----  
dev1      -/a          Virtual BLOCK Device    n/a           (unknown)       250.0 GiB     BLOCK  
dev2      -/b          Virtual BLOCK Device    n/a           (unknown)       10.0 GiB      BLOCK  
dev3      -/c          Virtual BLOCK Device    n/a           (unknown)       1.0 TiB       BLOCK  
-----
```


6. Add the metadata storage disks to the active tier:

```
# storage add tier active dev<n>
```

7. Create and enable the file system:

```
# filesystem create  
# filesystem enable
```

8. DDVE requires reliable time synchronization for object store communication. DDVE can synchronize time by using Amazon Time Sync Service or by configuring an NTP server.

Option	Description
Method 1 - Using Amazon Time Sync Service (recommended)	By default, DDVE uses Amazon Time Sync Service for time synchronization through a chrony client. DDVE does not require Internet access or configuration of security group rules to use this time synchronization service. Dell EMC recommends using the Amazon Time Sync Service.
Method 2 - Configuring NTP server (not recommended)	To override the default, you can configure an NTP server by running these commands: <ul style="list-style-type: none">ntp add timeserver 0.amazon.pool.ntp.orgntp enablentp sync <p> NOTE: ntp disable switches to the default time synchronization option (Amazon Time Sync Service).</p>

Results


The DDVE configuration is complete.

Configure the DDVE manually

This section describes how to manually configure the DDVE, e.g., updating elicense, setting the system passphrase, enabling the object-store feature and setting the object-store profile. These steps can be executed if the configuration wizard was skipped or at any point after the initial configuration.

Steps

1. Add the elicense by placing the license file under `/ddr/var/license`. Run the command `elicense update license.lic`

 **NOTE:** If the license file cannot be found in `/ddr/var` its content can be pasted directly on the console.

```
# elicense update license.lic  
Existing licenses:  
  
Capacity licenses:
```



```

##      Feature      Capacity      Type      State      Expiration Date      Note
--      -
1      CAPACITY      0.45 TiB      unexpired evaluation      active      n/a
--      -

Feature licenses:
##      Feature      Count      Type      State      Expiration
Date      Note
--      -
1      REPLICATION      1      unexpired evaluation      active      n/
a
2      DDBOOST      1      unexpired evaluation      active      n/
a
3      RETENTION-LOCK-GOVERNANCE      1      unexpired evaluation      active      n/
a
4      ENCRYPTION      1      unexpired evaluation      active      n/
a
--      -
-----

New licenses:

Capacity licenses:
##      Feature      Capacity      Type      State      Expiration Date      Note
--      -
1      CAPACITY      87.31 TiB      permanent (int)      active      n/a
--      -

Feature licenses:
##      Feature      Count      Type      State      Expiration Date      Note
--      -
1      DDBOOST      1      permanent (int)      active      n/a
2      ENCRYPTION      1      permanent (int)      active      n/a
3      REPLICATION      1      permanent (int)      active      n/a
--      -

** New license(s) will overwrite all existing license(s).

Do you want to proceed? (yes|no) [yes]: yes

eLicense(s) updated.

```

2. 2. Set the system passphrase by running the command `system passphrase set`.

```

# system passphrase set
Enter new passphrase:
Re-enter new passphrase:
Passphrases matched.
Passphrase is set.

```


3. 3. Enable object store using the command `storage object-store enable`.

```

# storage object-store enable
Object-store is enabled.

```

4. 4. Run the following command to create/modify the cloud profile: `# storage object-store profile set`. Enter the bucket name and import the Baltimore CyberTrust Root certificate to communicate with the object store.

 **NOTE:** For AWS GovCloud, profile creation will have an additional option to enable the FIPS endpoint.

```

# storage object-store profile set
A passphrase needs to be set on the system.
Enter new passphrase: <enter-passphrase-string-meeting-requirements>
Re-enter new passphrase: <re-enter-passphrase-string>
Passphrases matched.
The passphrase is set
DD VE is running in AWS. Role-based access will be used to access s3.
Enter the bucket name: <name-of-the-bucket>

```

```

Do you want to use the FIPS 140-2 endpoint (yes|no) [no]: no
Object-store endpoint needs the Baltimore CyberTrust Root
certificate to be imported.
Do you want to import that certificate with below fingerprint?
D4:DE:20:D0:5E:66:FC:53:FE:1A:50:88:2C:78:DB:28:52:CA:E4:74
(yes|no) [yes]:
Profile is set

```

Recovering DDVE with system headswap

The system headswap command recovers DDVE with head unit failure in AWS.

Prerequisites

System headswap between the same DDOS versions is recommended. When the same DDOS version not available, system headswap can be done with a higher DDOS version. The version check rules for RPM upgrade also apply.

Ensure that vNVRAM disk and Metadata disks from system A (original system) are available. These disks will be attached to the new instance B. If either vNVRAM disk or any metadata disk is not available, use the `system recovery from object-store` command instead.

Steps

1. Create instance B with Head Unit (root disk only) with the same instance type as instance A.
2. Attach the same role to instance B as that of instance A.
3. On instance A, make a note of the vNVRAM disk name (usually `sdb`). Use the same name when attaching the vNVRAM disk to instance B.

The screenshot shows the AWS Management Console interface. On the left is a navigation menu with categories like INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, LOAD BALANCING, and AUTO SCALING. The main panel displays the details for an EC2 instance named 'ddve_test' with Instance ID 'i-0489748d168805f8a'. The instance is in a 'running' state, using an 'm4.xlarge' instance type in the 'us-east-1a' availability zone. Below the instance summary, there are tabs for 'Description', 'Status Checks', 'Monitoring', and 'Tags'. The 'Description' tab is active, showing a detailed list of instance attributes. A red box highlights the 'Block devices' section, which lists the root device as '/dev/sda1' and a secondary block device as '/dev/sdb'.

Attribute	Value
Instance ID	i-0489748d168805f8a
Instance state	running
Instance type	m4.xlarge
Elastic IPs	-
Availability zone	us-east-1a
Security groups	ddve-priv-sg, view inbound rules, view outbound rules
Scheduled events	No scheduled events
AMI ID	hebbam1_atooos_ddve_7005 (ami-082fc1282390a563)
Platform	-
IAM role	ddrole-sharms62-bucket
Key pair name	ddve-bastion
Owner	383125126320
Launch time	September 9, 2019 at 2:42:02 AM UTC-7 (less than one hour)
Termination protection	False
Lifecycle	normal
Monitoring	basic
Public DNS (IPv4)	-
IPv4 Public IP	-
IPv6 IPs	-
Private DNS	ip-10-2-1-238.ec2.internal
Private IPs	10.2.1.238
Secondary private IPs	-
VPC ID	vpc-dfa786b1 (ddve-vpc)
Subnet ID	subnet-1440b74f (ddve-priv-sub-1a)
Network interfaces	eth0
Source/dest. check	True
T2/T3 Unlimited	-
EBS-optimized	True
Root device type	ebs
Root device	/dev/sda1
Block devices	/dev/sdb
Elastic Graphics ID	-

4. Detach the vNVRAM and metadata disks from the failed head unit.
5. Attach the vNVRAM disk to instance B. While attaching the vNVRAM disk, ensure that the name of the disk on instance B is same as that on instance A.

Attach Volume

Volume	vol-087f14f8fec5e0db1 (shefali_ddve_test_li_6) in us-east-1a
Instance	i-01153271e776ac63c in us-east-1a
Device	/dev/sdb Linux Devices: /dev/sdf through /dev/sdp

Note: Newer Linux kernels may rename your devices to /dev/xvdf through /dev/xvdp internally, even when shown in the details is /dev/sdf through /dev/sdp.

NOTE: Ensure that the vNVRAM disk is attached before attaching the metadata disks.

6. Attach the metadata disks to instance B.

7. Set the system passphrase.

NOTE: Set the passphrase to match system A, otherwise, the headswap fails.

```
# system passphrase set
Enter new passphrase:
Re-enter new passphrase:
Passphrases matched.
The passphrase is set.
```

8. Before executing the headswap command, ensure that system A is powered off. This step is required to detach the bucket from system A and make it available to be attached to system B.

9. Execute system headswap.

NOTE: The system will reboot during the headswap process.

```
# system headswap
This command returns the system back to its prior operational
conditions. The system will be rebooted before
resuming normal operations.
** If system passphrase was set on the old head, you will
   need to do one of the following after headswap completes:
   - unlock the filesystem           if you have encrypted data, or
   - set the system passphrase      if you don't have encrypted data
Are you sure? (yes|no) [no]: yes
ok, proceeding.
Please enter sysadmin password to confirm 'system headswap':
Restoring the system configuration, do not power off / interrupt
process ...
Broadcast message from root (Mon Apr 30 13:44:10 2018):
The system is going down for reboot NOW!
```

10. Verify the file system status after the headswap process completes.

```
# fileysys status
The filesystem is enabled and running.
```

NOTE:

- You may need to re-activate the license on the new instance if an unserved-mode license is used.
- The CLI elicense check-out and elicense check-in are used to obtain licenses from the DDVE.
 - If you experience an invalid key magic issue after a headswap, set the passphrase on the new DDVE system, and then perform the headswap `ddboost user revoke token-access sysadmin` command.
 - If the DDVE was attached to an AV-server and you experienced a certificate authentication issue after a headswap, detach and re-attach the DD from the AV-server. The AV-server regenerates the certificate and imports it to DD.

Recovering the system

The system recovery command recovers the DDVE system with head unit, vNVRAM disk, and metadata disk after a failure of one or more of these components.

About this task

If both vNVRAM disk and Metadata disks are available, then the `system headswap` command should be used instead.

Steps

1. Create instance B with the same configuration as instance A, including instance type, metadata disk capacity, and role.
2. Enable object-store:

```
# storage object-store enable
Object-store is enabled.
```


3. Set object-store profile:

- a. Set the passphrase to match system A, otherwise, the recovery fails to proceed.
- b. Set the same s3 bucket name from system A:

```
# storage object-store profile set
A passphrase needs to be set on the system.
Enter new passphrase: <enter-passphrase-string-meeting-requirements>
Re-enter new passphrase: <re-enter-passphrase-string>
Passphrases matched.
The passphrase is set
DDVE is running in AWS. Role-based access will be used to access s3.
    Enter the bucket name: <name-of-the-bucket>
    Object-store endpoint needs the Baltimore CyberTrust Root certificate to be
imported.
    Do you want to import that certificate with below fingerprint?
    D4:DE:20:D0:5E:66:FC:53:FE:1A:50:88:2C:78:DB:28:52:CA:E4:74 (yes|no) [yes]:
    Profile is set.
```

```
# storage object-store profile set
```

- c. Follow the rest of the CLI prompts.
4. Add EBS volumes to the active tier:

 **NOTE:** Add EBS volumes to match or exceed the capacity of system A .

```
# storage add dev3
Checking storage requirements...done
Adding dev3 to the active tier...done
Updating system information...done
dev3 successfully added to the active tier.
```

5. Run the system recovery precheck:


```
# system recovery precheck from object-store
Recovery precheck passed. Use start command to start the recovery.
```

6. Run the recovery:

```
# system recovery start from object-store
System recovery has started. Use status command to check the status.
```

7. Check the recovery status:

```
# system recovery status
System recovery is running: stage 2 of 6 (attaching object-store)
```

 **NOTE:** The system reboots during the recovery process.

8. Check that the filesys status after the recovery process completes:

```
# filesys status
The filesystem is enabled and running.
```

Administering DDVE

This chapter includes the following topics:

Topics:

- [Upgrade from M4 to M5 instance type](#)
- [Upgrading M5 instance type](#)
- [Extensions to DDOS for DDVE](#)
- [DDVE-only commands](#)
- [Modified DD OS commands](#)
- [Unsupported DD OS commands](#)
- [Troubleshooting performance issues](#)

Upgrade from M4 to M5 instance type

To benefit from performance improvements, you can upgrade an M4 instance type to the next generation M5 instance type.

Prerequisites

Ensure that:

- DDOS version is 7.2 or later. If the DDOS version is older, upgrade the DDOS version. Run the `system show version` command to check the DDOS version on the DDVE.
- The DDOS upgrade is successful.

Steps

1. To ensure a clean file system shutdown, run the `system poweroff` command.
2. From the AWS management console, change the instance type to one with the same or higher capacity.

Capacity (TB)	vCPU #, memory (GiB)	M4 instance type	M5 instance type
16	4, 16	m4.xlarge	m5.xlarge
32	8, 32	m4.2xlarge	m5.2xlarge
96	16, 64	m4.4xlarge	m5.4xlarge

NOTE: Alternatively, you can change the instance type with this command:

```
aws ec2 modify-instance-attribute --instance-id <instance-id> --instance-type
{"Value": "<M5 instance type>"}
```

For example:

```
aws ec2 modify-instance-attribute --instance-id i-03abf8df1da1bf061 --instance-type
{"Value": "m5.4xlarge"}
```

3. Enable the ena attribute by using this AWS command:


```
aws ec2 modify-instance-attribute --instance-id <instance_id> --ena-support
```
4. To verify that ena support is enabled for the instance, run this AWS command:


```
aws ec2 describe-instances --instance-ids <instance_id> --query
"Reservations[].Instances[].EnaSupport"
```
5. From the AWS management console, power on the DDVE.


6. On the DDVE, verify that the system is up, and ensure that the file system status is enabled and running.
7. To confirm that the instance type is an M5 instance type, run the `system vresource show current` command:

Upgrading M5 instance type

You can upgrade the current M5 instance type to higher capacity supported configuration.

About this task

For details about supported configurations, see [Storage size specifications](#) on page 49.

 **NOTE:** Instance upgrade is not supported for DDVE with block storage as it supports a maximum capacity of 16 TB.

Steps

1. Power off the system using the `system poweroff` command.
From the AWS console, check that the DDVE instance is in the stopped state.
2. Select **Action** > **Instance Settings** > **Change Instance Type**.
3. Select the new instance type and click **Apply**.
4. Power on the DDVE from the AWS console.
5. Once the DDVE is powered on, run the command `system vresource show` to verify the new instance configuration.

Extensions to DDOS for DDVE

Several DDOS commands are supported on the DDVE platform only. This section describes these commands.

perf

Collect and show DDVE performance statistics.

```
perf disable trace event-regex [module {default | ddfs}]
```

Disable tracing of specified events.

```
perf enable trace event-regex [module {default | ddfs}]
```

Enable tracing of the specified events.

```
perf start histogram [module {default | ddfs}]
```

Start collecting performance histograms. This command may reduce performance marginally.

```
perf start stats
```

Start printing statistics. This command may reduce performance marginally.

```
perf start trace [allow-wrap] [module {default | ddfs}]
```

Start tracing events. This command may reduce performance marginally.

```
perf status trace event-regex [module {default | ddfs}]
```

Shows whether tracing is enabled or disabled for the specified events.

```
perf stop histogram histogram-filename [module {default | ddfs}]
```

Stop collecting histograms and write the collected histograms to the specified file.

```
perf stop stats
```

Stop printing statistics.

```
perf stop trace trace-filename [module {default | ddfs}]
```

Stop tracing events and write the collected traces to the specified file.

System vresource

Display details about the virtual CPU and memory resources on the DDVE.

`system vresource show [current | requirements]`

```
# system vresource show requirements
Active Tier      Cloud Tier      Instance
Capacity (TB)   Capacity (TB)   Type
-----
          16          n/a          m5.xlarge
          32          n/a          m5.2xlarge
          96          n/a          m5.4xlarge
         256          n/a          m5.8xlarge
-----
** The maximum allowed system capacity for active tier on block storage is 16 TB
```

DDVE-only commands

The following commands only work on DDVE and are not supported on physical DD systems.

Table 4. DDVE-only commands

Command	Description
<code>elicense checkout feature-license <feature-name-list></code>	Allows user to check out the features of licenses for License Server installation
<code>elicense checkout capacity-license <feature-name> value <n> {TB GB}</code>	Allows user to check out the capacity of licenses for License Server installation. Here is sample output: <code>sysadmin@localhost# elic checkout capacity-license capacity value 10 TB</code> Checking out CAPACITY license willl also checkout available feature licenses. An addition 10 TB CAPACITY license will be checked out. 10 TB additional CAPACITY license has been checked out. License(s) have been checked out for REPLICATION, DDBOOST, ENCRYPTION. Total 10 TB CAPACITY license is now available on this system.
<code>elicense checkin {<feature-name-list> all}</code>	Allows user to check in features for licenses for License Server installation
<code>elicense license-server set server {<ipaddr> <hostname>} port <port-number></code>	
<code>elicense license-server reset</code>	Returns DDVE to factory license settings.
<code>elicense license-server show</code>	
<code>filesys show space tier active local-metadata</code>	Displays the usage for the metadata storage. NOTE: Some portion of the disk space is reserved for internal metadata, such as index. The amount of reserved space is based on the maximum capacity of the platform and not on licensed capacity.
<code>net hosts add</code>	Two DDVEs in different regions cannot resolve each other's hostname. Run this command to add a host list entry.
<code>storage object-store enable</code>	Enables the object-store feature for DDVE.
<code>storage object-store disable</code>	Disables the object-store feature for DDVE.
<code>storage object-store profile set</code>	Configures the object-store access profile.
<code>storage object-store profile show</code>	Displays the object-store access profile.

Table 4. DDVE-only commands (continued)

Command	Description
<code>storage object-store profile status</code>	This CLI lists the object-store profile information set on the DDVE.
<code>system vresource show [requirements]</code>	Displays the file system capacity, the number of virtual CPUs, and the amount of memory assigned to the virtual machine running the DDVE instance. The <code>requirements</code> option displays the physical storage requirements for DDVE.

Modified DD OS commands

The behavior of the following commands is modified on the DDVE platform:

Table 5. Modified DD OS commands

Command	Changes
<code>alert</code>	The <code>tenant-unit</code> parameter is not supported.
<code>compression</code>	The <code>tenant-unit</code> parameter is not supported.
<code>config setup show</code>	Arguments for configuring features not available in DDVE have been removed.
<code>ddboost clients show active</code>	The <code>tenant-unit</code> parameter is not supported.
<code>ddboost file-replication show active</code>	The <code>tenant-unit</code> parameter is not supported.
<code>ddboost file-replication show detailed-file-history</code>	The <code>tenant-unit</code> parameter is not supported.
<code>ddboost file-replication show file-history</code>	The <code>tenant-unit</code> parameter is not supported.
<code>ddboost option reset</code>	The <code>fc</code> parameter is not supported.
<code>ddboost option show</code>	The <code>fc</code> parameter is not supported.
<code>ddboost storage-unit create</code>	The <code>tenant-unit</code> parameter is not supported.
<code>ddboost storage-unit modify</code>	The <code>tenant-unit</code> parameter is not supported.
<code>ddboost storage-unit show</code>	The <code>tenant-unit</code> parameter is not supported.
<code>ddboost streams show active</code>	The <code>tenant-unit</code> parameter is not supported.
<code>ddboost streams show history</code>	The <code>tenant-unit</code> parameter is not supported.
<code>disk rescan</code>	The <code><enlclosure-ID>.<disk-ID></code> parameter is not supported.
<code>disk show state</code>	DDVE system disks show the <code>System Dev</code> state.
<code>disk show stats</code>	The DDVE format for this command is <code>disk show stats [dev <n>]</code>
<code>disk status</code>	The <code>Spare</code> row has been removed from the output. The <code>System</code> row has been added.
<code>enclosure show all</code>	The <code>[<enclosure>]</code> parameter is not supported.
<code>enclosure show controllers</code>	The <code>[<enclosure>]</code> parameter is not supported.
<code>enclosure show cpus</code>	The <code>[<enclosure>]</code> parameter is not supported.
<code>enclosure show io-cards</code>	The <code>[<enclosure>]</code> parameter is not supported.

Table 5. Modified DD OS commands (continued)

Command	Changes
<code>enclosure show memory</code>	The [<i><enclosure></i>] parameter is not supported.
<code>filesystem encryption keyes delete</code>	The [tier {active archive} archive-unit <i><unit-name></i>] parameter is not supported.
<code>filesystem encryption keys show</code>	The [tier {active archive} archive-unit <i><unit-name></i>] parameter is not supported.
<code>filesystem fastcopy</code>	The [retention-lock] parameter is supported with DDVE. Retention lock compliance mode is not supported for any DDVE.
<code>filesystem show compression</code>	The [tier {active archive} archive-unit <i><unit-name></i>] parameter is not supported.
<code>filesystem show space</code>	The [tier {active archive} archive-unit <i><unit-name></i> arcjove-unit {all <i><unit-name></i> }] parameter is not supported.
<code>mtree create</code>	The tenant-unit parameter is not supported.
<code>mtree list</code>	The tenant-unit parameter is not supported.
<code>mtree show compression</code>	The tenant-unit and tenant-unit parameters are not supported.
<code>mtree show performance</code>	The tenant-unit parameter is not supported.
<code>net create interface</code>	The <i><virtual-ifname></i> parameter is not supported.
<code>net destroy</code>	The <i><virtual-ifname></i> parameter is not supported.
<code>perf</code>	The vtl option is not supported on any perf command.
<code>storage add</code>	The enclosure and disk parameters are not supported.
<code>storage remove</code>	The enclosure and disk parameters are not supported.
<code>storage show</code>	The archive option is not supported.
<code>system show stats</code>	NVRAM statistics are not reported, because DDVE systems do not have physical NVRAM.
<code>quota</code>	The tenant-unit parameter is not supported.
<code>replication</code>	MTree replication is the only type of replication supported.
<code>snapshot</code>	The tenant-unit parameter is not supported.

Unsupported DD OS commands

The following DD OS commands and command options are not supported on the DDVE platform.

Table 6. Unsupported commands and command options

Unsupported command or command option	Notes
<code>adminaccess https generate certificate</code>	Deprecated. Use <code>adminaccess certificate generate</code> instead.
<code>alerts add</code>	Deprecated. Use <code>alerts notify-list add</code> instead.
<code>alerts del</code>	Deprecated. Use <code>alerts notify-list del</code> instead.

Table 6. Unsupported commands and command options (continued)

Unsupported command or command option	Notes
alerts notify-list option set <i>group-name</i> tenant-alert-summary {enabled disabled}	
alerts notify-list option reset <i>group-name</i> tenant-alert-summary	
alerts reset	Deprecated. Use alerts notify-list reset instead.
alerts show alerts-list	Deprecated. Use alerts notify-list show instead.
alerts test	Deprecated. Use alerts notify-list test instead.
archive	
authorization	
autosupport display	Deprecated. Use autosupport show report instead.
autosupport reset support-list	Deprecated. Use autosupport reset { all alert-summary asup-detailed support-notify } instead.
autosupport show support-list	Deprecated. Use autosupport show { all asup-detailed alert-summary support-notify } instead.
cifs set authentication nt4	Deprecated. Use cifs set authentication active-directory instead.
cluster	
ddboost fc	
ddboost option reset fc	
ddboost option set distributed-segment-processing disabled	Turning off distributed segment processing (DSP) with this DDBoost command is not supported for DDVE on DD OS 6.1.2.x.
ddboost option show	Turning off DSP with this DDBoost command is not supported for DDVE on DD OS 6.1.2.x.
ddboost option show fc	
ddboost show image-duplication	Deprecated. Use ddboost file-replication show instead.
ddboost user option set user default-tenant-unit <i>tenant-unit</i>	
ddboost user option reset user [default-tenant-unit]	
disk add devdisk-id [spindle-group 1-16]	Deprecated. Use storage add instead.
disk add enclosure <i>enclosure-id</i>	Deprecated. Use storage add instead.
disk benchmark start	Not supported by DDVE in cloud
disk benchmark show	Not supported by DDVE in cloud
disk benchmark stop	Not supported by DDVE in cloud
disk benchmark watch	Not supported by DDVE in cloud
disk expand	Deprecated. Use storage add instead.
disk failenclosure-id.disk-id	
disk multipath	

Table 6. Unsupported commands and command options (continued)

Unsupported command or command option	Notes
<code>disk port</code>	
<code>disk rescan [enclosure-id.disk-id]</code>	
<code>disk show detailed-raid-info</code>	Deprecated. Use <code>disk show state</code> and <code>storage show</code> instead.
<code>disk show failure-history</code>	
<code>disk show performance</code>	Not supported by DDVE in cloud
<code>disk show raid-info</code>	Deprecated. Use <code>disk show state</code> and <code>storage show</code> instead.
<code>disk show reliability-data</code>	
<code>disk disk show stats</code>	Not supported by DDVE in cloud
<code>disk unfail</code>	
<code>enclosure beacon</code>	
<code>enclosure show all [enclosure]</code>	This command is supported, but not with the <i>enclosure</i> argument.
<code>enclosure show chassis</code>	
<code>enclosure show controllers enclosure</code>	This command is supported, but not with the <i>enclosure</i> argument.
<code>enclosure show cpus [enclosure]</code>	This command is supported, but not with the <i>enclosure</i> argument.
<code>enclosure show fans</code>	
<code>enclosure show io-cards [enclosure]</code>	This command is supported, but not with the <i>enclosure</i> argument.
<code>enclosure show memory [enclosure]</code>	This command is supported, but not with the <i>enclosure</i> argument.
<code>enclosure show nvram</code>	
<code>enclosure show powersupply</code>	
<code>enclosure show summary</code>	
<code>enclosure show temperature-sensors</code>	
<code>enclosure show topology</code>	
<code>enclosure test topology</code>	
<code>filesystems archive</code>	
<code>filesystems clean update-stats</code>	Deprecated. Use <code>filesystems show space</code> instead.
<code>filesystems encryption</code>	
<code>filesystems encryption passphrase change</code>	Deprecated. Use <code>system passphrase change</code> instead.
<code>filesystems retention-lock</code>	Deprecated. Use <code>mtree retention-lock</code> instead.
<code>filesystems show compression tier</code>	The <code>tier</code> option is not supported.
<code>filesystems show history</code>	Deprecated. Use <code>filesystems show compression daily</code> instead.
<code>ha create</code>	Not supported by DDVE in cloud
<code>ha destroy</code>	Not supported by DDVE in cloud

Table 6. Unsupported commands and command options (continued)

Unsupported command or command option	Notes
<code>ha status</code>	Not supported by DDVE in cloud
<code>ha failover</code>	Not supported by DDVE in cloud
<code>ha online</code>	Not supported by DDVE in cloud
<code>ha offline</code>	Not supported by DDVE in cloud
<code>license</code>	The <code>license</code> commands are not supported because DDVE uses new <code>elicense</code> commands.
<code>mtree show compression mtree_path tier</code>	
<code>net aggregate</code>	
<code>net config ifname type cluster</code>	
<code>net create interface virtual-ifname</code>	
<code>net create interface physical-ifname vlan vlan-id</code>	
<code>net create virtual vethid</code>	
<code>net destroy virtual-ifname</code>	
<code>net destroy vlan-ifname</code>	
<code>net failover</code>	
<code>net modify virtual-ifname bonding {aggregate failover}</code>	
<code>net set portnaming</code>	
<code>ndmp</code>	
<code>ndmpd</code>	
<code>nfs option disable report-replica-as-writable</code>	Deprecated. Use <code>filesystem option disable report-replica-as-writable</code> instead.
<code>nfs option enable report-replica-as-writable</code>	Deprecated. Use <code>filesystem option enable report-replica-as-writable</code> instead.
<code>nfs option reset report-replica-as-writable</code>	Deprecated. Use <code>filesystem option reset report-replica-as-writable</code> instead.
<code>nfs option show report-replica-as-writable</code>	Deprecated. Use <code>filesystem option show report-replica-as-writable</code> instead.
<code>perf * module vtl</code>	
<code>san</code>	
<code>shelf migration start</code>	Not supported by DDVE in cloud
<code>shelf migration status</code>	Not supported by DDVE in cloud
<code>shelf migration suspend</code>	Not supported by DDVE in cloud
<code>shelf migration resume</code>	Not supported by DDVE in cloud
<code>shelf migration precheck</code>	Not supported by DDVE in cloud
<code>shelf migration option</code>	Not supported by DDVE in cloud
<code>shelf migration finalize</code>	Not supported by DDVE in cloud
<code>shelf migration show history</code>	Not supported by DDVE in cloud

Table 6. Unsupported commands and command options (continued)

Unsupported command or command option	Notes
<code>snapshot add schedule name [days days] time time [,time...] [retention period]</code>	Deprecated. Use <code>snapshot schedule create</code> instead.
<code>snapshot add schedule name [days days] time time every mins [retention period]</code>	Deprecated. Use <code>snapshot schedule create</code> instead.
<code>snapshot add schedule name [days days] time time-time [every hrs mins] [retention period]</code>	Deprecated. Use <code>snapshot schedule create</code> instead.
<code>snapshot del schedule {name all}</code>	Deprecated. Use <code>snapshot schedule destroy</code> instead.
<code>snapshot modify schedule name {[days days] time time [,time...] [retention period]}</code>	Deprecated. Use <code>snapshot schedule modify</code> instead.
<code>snapshot modify schedule name {[days days] time time every {mins none} [retention period]}</code>	Deprecated. Use <code>snapshot schedule modify</code> instead.
<code>snapshot modify schedule name {[days days] time time-time [every {hrs mins none}] [retention period]}</code>	Deprecated. Use <code>snapshot schedule modify</code> instead.
<code>snapshot reset schedule</code>	Deprecated. Use <code>snapshot schedule reset</code> instead.
<code>snapshot show schedule</code>	Deprecated. Use <code>snapshot schedule show</code> instead.
<code>storage add enclosure enclosure-id</code>	
<code>storage add disk enclosure-id.disk-id</code>	
<code>storage remove enclosure enclosure-id</code>	
<code>storage remove disk enclosure_id.disk-id</code>	
<code>system firmware</code>	
<code>system option set console</code>	
<code>system retention-lock</code>	
<code>system sanitize</code>	
<code>system show anaconda</code>	
<code>system show controller-inventory</code>	
<code>system show nvram</code>	
<code>system show nvram-detailed</code>	
<code>system show oemid</code>	
<code>system upgrade continue</code>	
<code>user</code>	
<code>user change priv</code>	Deprecated, with no replacement.
<code>vserver config set host</code>	Not supported by DDVE in cloud
<code>vserver config reset</code>	Not supported by DDVE in cloud
<code>vserver config show</code>	Not supported by DDVE in cloud
<code>vserver config perf-stats start</code>	Not supported by DDVE in cloud
<code>vserver config perf-stats stop</code>	Not supported by DDVE in cloud
<code>vserver config perf-stats status</code>	Not supported by DDVE in cloud
<code>vtl lunmask</code>	Deprecated. Use <code>vtl group</code> instead.

Table 6. Unsupported commands and command options (continued)

Unsupported command or command option	Notes
<code>vtl lunmask add</code>	Deprecated. Use <code>vtl group add</code> instead.
<code>vtl lunmask del</code>	Deprecated.
<code>vtl lunmask show</code>	Deprecated. Use <code>vtl group show</code> instead.

Troubleshooting performance issues

You can check DDVE performance statistics as follows:

- With native tools in AWS

You can also use the following to monitor benchmark performance:

- `perf`

[Extensions to DDOS for DDVE](#) on page 39 provides more information about commands.

CPU Performance

The two key statistics for CPU performance are:

- CPU usage—CPU usage as a percentage during the interval
- CPU ready—The percentage of time that the virtual machine was ready, but could not get scheduled to run on the physical CPU. This counter might not be displayed by default.

If these counters are high, there may be a performance problem on the hypervisor host.

Memory Performance

- Memory swapping—The key statistic for memory performance, which is the current amount of guest physical memory swapped out to the virtual machine's swap file.

Virtual Disk Performance

The key statistics for virtual disk performance are:

- I/O throughput—A decrease in these values indicates a performance issue.
- I/O latency—An increase in read and write latency values indicates a performance problem.

Failed commands—An increase in the average number of outstanding read and write requests indicates a performance problem.

Best Practices for Working with DDVE in the Cloud

This chapter includes the following topics:

Topics:

- [ASUP configuration](#)
- [AWS licensing](#)
- [Storage best practices](#)
- [Security best practices](#)

ASUP configuration

We recommend enabling AutoSupport (ASUP) in DDVE. Although Experience, Secure Remote Services (ESRS) is not yet supported in AWS, you can use the email transfer server to transfer ASUP files.

About this task

Set up the following items to ensure that ASUPs and alert emails from the DDVE instance are sent to Dell EMC.

1. Administrator: Specify a password and email address for the administrator.
2. Email/location: Specify the mail sever to use to send outgoing alert and ASUPs to recipients. Recipients are subscribers to groups. A default group is created that contains the email addresses of the administrator and a Dell EMC email address, `autosupportalert@autosupport.datadomain.com`. The location field is for information only.
3. Review the summary carefully. The default email address for alerts and autosupport emails is `autosupportalert@autosupport.datadomain.com`. A detailed autosupport and an alert summary are scheduled to run daily at 6:00 AM system time.

AWS licensing

The DDVE license is node locked which means the same license cannot be used on multiple DDVE instances. To facilitate DDVE license management, we recommend using served-mode licenses if multiple DDVEs are to be deployed.

NOTE:

- The DDVE license might become invalid after removing the first NIC `ethV0`.
- In the case of a head swap, the license will continue to work on new DDVE instance if served-mode licenses are used, otherwise you need to re-activate the license.
- You may create a new DDVE instance from an AWS snapshot. The license is automatically checked out from the license server on the new instance if served-mode licenses are used, as long as the license server has sufficient licenses for this new instance to check out. Otherwise you need to re-activate the license.

Storage best practices

Use the appropriate storage type

Use GP2 EBS volumes for the root disk, NVRAM disk, and metadata disks.

Object storage specifications

The following table lists the supported instance types and their storage configuration for object storage.

Metadata disk storage is recommended to be 10% of the total capacity. Each metadata disk is recommended to be 1 TiB.

Table 7. Storage size specifications

DDVE configuration	Instance type	Root disk (GP2)	NVRAM disk (GP2)	Metadata disk (GP2)	Metadata disks required
16 TB	M5.xlarge	250 GiB	10 GiB	1024 GiB	1-2
32 TB	M5.2xlarge	250 GiB	10 GiB	1024 GiB	1-4
96 TB	M5.4xlarge	250 GiB	10 GiB	1024 GiB	1-10
256 TB	M5.8xlarge	250 GiB	10 GiB	2048 GiB	1-13

NOTE:

- If the incorrect instance type is used, the system displays an alert for an unsupported virtual hardware configuration.
- The metadata requirements that are listed above are based on a 10x deduplication ratio and a 2x compression ratio. For workloads with a higher deduplication ratio, more metadata storage is required.
- The maximum number of metadata disks that you can add to a DDVE instance in AWS is 24.

Block storage specifications

The following table lists the instance types and storage types that are required for block storage.

Table 8. Storage configuration types for DDVE in AWS (block store)

DDVE configuration	Instance type	Root disk type/size	NVRAM disk type/size	Data disk type/size
16 TB	M5.xlarge	GP2/250 GB	GP2/10 GB	GP2/1024 GB

NOTE:

- DDVE with block storage supports a maximum capacity of 16 TB. The recommended size of each data disk is one TiB.
- If the incorrect instance type is used, the system displays an alert for an incorrect virtual hardware configuration.

Table 9. Supported stream and Mtree counts

System capacity	Instance type	vCPU	Memory (GiB)	Max Mtree	Stream counts				
					Read	Write	Replication in	Replication out	Combined
16 TB	M5.xlarge	4	16	6	30	45	45	42	60
32 TB	M5.2xlarge	8	32	14	50	90	90	82	90
96 TB	M5.4xlarge	16	64	32	50	180	180	100	180
256 TB	M5.8xlarge	32	128	128	110	540	540	220	540

Metadata disk storage expansion notes

Dell EMC recommends to use 10% of the system capacity as the metadata storage, where each metadata disk size is one TiB. This metadata storage recommendation is based on 10X deduplication ratio and 2X compression. For workloads with a higher deduplication ratio, more metadata storage may be required. If metadata storage usage exceeds 80%, an alert is generated. Add a metadata disk to the DDVE immediately to avoid running out of space.

The *DD OS Administration Guide* provides a procedure for expanding storage. Dell EMC recommends that you always use 1 TiB metadata disks.

Spindle group

You are not required to specify a spindle group when adding metadata disks. The spindle group assignment is balanced automatically when adding storage. Do not set or change the spindle group settings manually. Run the `storage show all` command to verify that each data volume is assigned to a different spindle group.

Object storage bucket configuration notes

- The bucket that is provided during file system creation must be empty, otherwise file system creation fails.
- When the file system is destroyed, the associated bucket and the objects it contains are not automatically deleted or removed. The bucket must be intentionally deleted to avoid incurring the cost for the content stored in the bucket.
- Do not enable S3 versioning on the bucket. Doing so incurs additional cost because older versions of the objects are retained, although they are removed by the GC cycles.
- Do not configure any life-cycle policy on the bucket as it might result in loss of critical data.

Converting from evaluation to production

Rather than convert an evaluation version of DDVE to a production version, Dell EMC recommends a fresh deployment. If you decide to convert from an evaluation version to production version, Dell EMC recommends that you:

- Destroy the existing file system
- Delete any small data disk (not the root or NVRAM disks)
- Configure new disks according to the recommendations in this guide

Security best practices

Avoid Public IP address

To prevent brute force attacks on the DDVE, it must not be configured with a public IP address.


Secure access

The following table illustrates the different authentication methods that are supported by DDVE.

Table 10. Access Types and Authentication

Access Type	Authentication Methods
GUI	username/password X509 certificates
SSH	username/password
	SSH key pair
REST API	username/password X509 certificates

For better security, we recommend you disable the username/password based user authentication. If the username/password based authentication is desired, we recommend that you configure a stronger password.

 **NOTE:** Password based login should not be disabled if you want to configure Avamar Virtual Edition, NetWorker, or other backup software to connect to DDVE in AWS, because password authentication is used for communication between them.

Because AWS is a public cloud, pay attention to the security in your deployment. We suggest these best practices:

- Use public key based authentication for SSH access
- Use certificate based authentication for DDSM access
- Do not configure public IP for DDVE in AWS, if possible
- Use external KMIP server to store encryption keys
- Enable encryption for DDFS and replication

After a DDVE deployment from the market place, DDVE SSH login with a username and password is enabled. The default password for the sysadmin user is the EC2 instance ID of the DDVE instance. At the first login, a password change is required. The EC2 key access pair associated with the sysadmin user is an optional alternative to username and password authentication.

IP Tables feature

After protecting the DDVE using secure setup, within the DDVE you can filter the network traffic that enters by using the `iptables` feature. For more configuration information, see the DD OS 6.2 Command Reference Guide's Net Filter section.

Security rules settings

Since the DDVE in AWS is always running in a VPC, the VPC should be configured so that only required and trusted clients have access to the DD system. The following tables show the TCP and UDP ports that are used by the DD system for inbound and outbound traffic, and which service makes use of them. Consider the following information when configuring VPC firewall rules. For additional information, see [Amazon EC2 Security Groups for Linux Instances](#).

Inbound rules

The following are the inbound ports used by DDVE.

Table 11. Inbound ports used by DDVE

Port	Service	Description
TCP 22	SSH	Used for SSH (CLI) access and for configuring DDVE.
TCP 443	HTTPS	Used for DDSM (GUI) access and for configuring DDVE.
TCP 2049	DD Boost/NFS	Main port used by NFS - can be modified using the <code>nfs set server-port</code> command which requires SE mode.
TCP 2051	Replication/DD Boost/ Optimized Duplication	Used only if replication is configured (run <code>replication show config</code> command on DD system to determine). This port can be modified using <code>replication modify</code> .
TCP 3009	SMS (system management)	Used for managing a system remotely using DDSM. This port cannot be modified. This port will also need to be opened if you plan to configure replication from within the DDSM, since the replication partner needs to be added to the DDSM.

Depending on the protocol that is used to backup data to DDVE, additional ports are enabled with inbound firewall rules.

Outbound rules

The following are the outbound ports that are used by DDVE.

Table 12. Outboard ports used by DDVE

Port	Service	Description
UDP 123	NTP	Used by the DD system to synchronize to a time server.
TCP 443	HTTPS	Used for DDVE to be able to communicate with outside services.
TCP 2049	DD Boost/NFS	Main port used by NFS - can be modified using the <code>nfs set server-port</code> command which requires SE mode.
TCP 2051	Replication/DD Boost/ Optimized Duplication	Used only if replication is configured (run <code>replication show config</code> on DD system to determine). This port can be modified using <code>replication modify</code> .

Table 12. Outboard ports used by DDVE (continued)

TCP 3009	SMS (system management)	Used for managing a system remotely using DDSM. This port cannot be modified. This port will also need to be opened if you plan to configure replication from within the DDSM, as the replication partner needs to be added to the DDSM.
----------	-------------------------	--

Depending on the other applications/services that are being used, additional ports shall be enabled for outbound firewall rules.

Networking Best Practices for DDVE in the Cloud

This chapter includes the following topics:

Topics:

- [Network setup in AWS](#)
- [Network infrastructure setup](#)

Network setup in AWS

VPC Architecture

We recommend you use public or private subnet architecture to deploy the DDVE in private subnet. It will secure the DDVEs (VMs) with the appropriate use of various VPC components such as route tables, access control lists, security groups, etc.

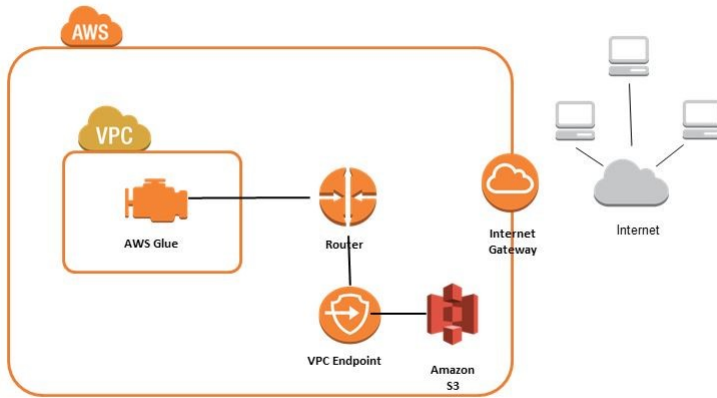
Public IP address

Due to security considerations and in order to protect the DDVE from potential attacks over open internet, the DDVE MUST NOT be exposed using Public IP directly over internet. It is highly recommended that you use VPN connections between different geographical regions (VPCs). For example, the replication between different VPCs, different cloud regions, cloud to on-premise and vice versa can be used via the secure VPN connection.

Object store connectivity

The DDVE object store feature needs connectivity to its object storage, such as to the S3 bucket. The object store communication is over https, so the outbound security group setting must allow communication over port 443. There are different ways to enable DDVE connectivity to the object store. Out of the following three we recommend only the third option (Using VPC endpoint).

- Using the public IP from the public subnet: should not be used
- Using NAT (Network Address Translation): If the private subnet is configured to use NAT, then DDVE will be able to communicate to object store over NAT.
- We strongly recommend using VPC endpoint for accessing the Amazon S3. It does not require the DDVE to have a public IP address to communicate to S3, it uses the private IP address instead. (In this case, an internet gateway, NAT, or virtual private gateway are not needed to access S3). This method also allows the traffic to the S3 endpoint to stay within the Amazon network and will be routed internally to S3.



NOTE:

- Refer to [Role based access for S3 object store](#) for configuring the DDVE to access the S3 bucket securely.
- The S3 bucket that was created for DDVE use, MUST be in the same region where DDVE is running.
- For information see [Amazon AWS documentation](#).

Network infrastructure setup

This section describes security group restrictions for AWS.

Security groups

The security groups restrict access to an instance based on

1. Port
2. IP range
3. Security group (its own or another)

Inbound control

The security groups are stateful which means that the responses to the inbound traffic will be allowed to go out regardless of outbound rules. The following are the inbound ports that are allowed for DDVE.

Table 13. DDVE Inbound Ports

Port	Service	Description
TCP 22	SSH	Used for SSH (CLI) access and for configuring DDVE.
TCP 443	HTTPS	Used for DDSM (GUI) access and for configuring DDVE.
TCP 2049	DD Boost/NFS	Main port used by NFS - can be modified using the <code>nfs set server-port</code> command which requires SE mode.
TCP 2051	Replication/DD Boost/Optimized Duplication	Used only if replication is configured (run <code>replication show config on DD system</code> to determine). This port can be modified using <code>replication modify</code> .
TCP 3009	SMS (system management)	Used for managing a system remotely using DD System Manager. This port cannot be modified. This port is used only on DD systems running DD OS 4.7.x or later. This port will also need to be opened if you plan to configure

Table 13. DDVE Inbound Ports (continued)

Port	Service	Description
		replication from within the DD System Manager, as the replication partner needs to be added to the DD System Manager.

Depending on the protocol that is used to backup data to DDVE, additional ports will be allowed with inbound security group rules.

Outbound control

As stated earlier the security groups are stateful, which means that if a request is allowed to be sent out of a DDVE, its responses will be allowed regardless of inbound rules. The following are the outbound ports that shall be allowed for DDVE.

Table 14. DDVE Outbound Ports

Port	Service	Description
UDP 123	NTP	Used by the DD system to synchronize to a time server.
TCP 443	HTTPS	Used for DDVE to be able to communicate with Object store (S3).
TCP 2049	DD Boost/NFS	Main port used by NFS - can be modified using the <code>nfs set server-port</code> command which requires SE mode.
TCP 2051	Replication/DD Boost/Optimized Duplication	Used only if replication is configured (<code>run replication show config</code> on DD system to determine). This port can be modified using <code>replication modify</code> .
TCP 3009	SMS (system management)	Used for managing a system remotely using DD System Manager. This port cannot be modified. This port is used only on DD systems running DD OS 4.7.x or later. This port will also need to be opened if you plan to configure replication from within the DD System Manager, as the replication partner needs to be added to the DD System Manager.

Depending on the other applications/services that are being used, additional ports shall be allowed.

Installing and Configuring DDVE on Block Storage in the Cloud

This chapter includes the following topics:

Topics:

- [Overview of DDVE on block storage](#)
- [Configuring DDVE on block storage with DD System Manager](#)

Overview of DDVE on block storage

DDVE on block storage provides enterprise customers and service providers who are running applications in the public cloud with a deduplication data protection appliance that provides object storage efficiency and ease of management.

DDVE on block storage supports:

- Backup and restore using active tier data into cloud block storage while DDVE is running in the cloud.
- DD System Manager to configure, manage, and monitor DDVE on block storage.
- DD Management Center for multisystem management of DDVE systems in the cloud on block storage.

Configuring DDVE on block storage with DD System Manager


You can use the DD System Manager to configure DDVE as an active tier on a block storage system.

About this task

Use the Configuration wizard to configure the active tier and create the file system on the DDVE instance.

Steps

1. Log in as sysadmin with the password **Ec2<DDVE-instance-ID>**.
2. To configure the active tier on block storage, ensure that the **Enable Object Store** checkbox is cleared and click **Next**.
3. Add the block storage attached to the DDVE to the active tier.

 **NOTE:** For block storage solution, the maximum supported storage capacity is 16 TB.

4. Review the summary and select **Submit** to create the file system and enable it.
5. To view the space usage and availability details for the block storage, select **Data Management > File System**.
6. To configure or update the eLicense on the DDVE instance, select **Licenses > Replace Licenses**.
7. To relaunch the configuration wizard, select **Maintenance > Configure System > Configure System**.