<table>
<thead>
<tr>
<th>CONTENTS</th>
</tr>
</thead>
</table>

Revision history 5

Preface 7

Chapter 1 Getting Started 9
   Purpose of this guide ................................................................. 10
   Audience ......................................................................................... 10
   Prerequisites, limitations, and resources ........................................ 10
   Architecture overview .................................................................. 11

Chapter 2 Introducing DDVE 13
   Introducing DDVE ......................................................................... 14
   DDVE cloud features .................................................................... 14

Chapter 3 Deploying DDVE 17
   Preparing your environment to deploy DDVE on AWS .................. 18
      Create an S3 bucket ................................................................. 18
      Set up role-based access to the AWS object store .................. 19
   Deploying DDVE in AWS ............................................................ 22
      Deploying DDVE using a Cloud Formation Template ............ 22
      Deploying DDVE manually from the AWS console ............... 25

Chapter 4 Completing Initial DDVE Configuration 31
   Configuring DDVE on AWS ......................................................... 32
      Using the DD System Manager to configure DDVE ............... 32
      Using the CLI to configure the DDVE ................................. 35
   Recovering DDVE with system headswap .................................. 39
   Recovering the system ............................................................... 41

Chapter 5 Administering DDVE 43
   Adding virtual storage ............................................................... 44
      Configuring spindle groups .................................................... 44
   Extensions to DDOS for DDVE .................................................... 44
      perf ....................................................................................... 44
      system vresource ................................................................. 45
   DDVE-only commands .............................................................. 45
   Modified DD OS commands ...................................................... 47
   Unsupported DD OS commands ................................................ 49
   Troubleshooting performance issues ....................................... 54

Appendix A Best Practices for Working with DDVE in the Cloud 57
   ASUP configuration ................................................................. 58
   AWS licensing ........................................................................... 58
Contents

Storage best practices........................................................................................................58
Security best practices.......................................................................................................60

Appendix B  Networking Best Practices for DDVE in the Cloud 63
Network setup in AWS........................................................................................................64
Network infrastructure setup...............................................................................................65
Setting up NTP time synchronization in AWS....................................................................66

Appendix C  Installing and Configuring DDVE on Block Storage in the Cloud 67
Overview of DDVE on block storage..................................................................................68
Configuring DDVE on block storage with DD System Manager.......................................68
## Revision history

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>05</td>
<td>March 2020</td>
<td>Editorial updates</td>
</tr>
<tr>
<td>04</td>
<td>January 2020</td>
<td>Editorial updates</td>
</tr>
<tr>
<td>03</td>
<td>October 2019</td>
<td>Editorial updates</td>
</tr>
<tr>
<td>02</td>
<td>March 2019</td>
<td>Editorial updates</td>
</tr>
<tr>
<td>01</td>
<td>December 2018</td>
<td>Initial Publication (with DD OS 6.2.0.5)</td>
</tr>
</tbody>
</table>
Preface

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.
  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](https://support.emc.com).

**Technical support**
For technical support of this release of DDVE, go to Online Support at [https://support.emc.com](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](mailto:DPAD.Doc.Feedback@emc.com).
CHAPTER 1
Getting Started

This chapter includes the following topics:

- Purpose of this guide ............................................................................................................. 10
- Audience ................................................................................................................................ 10
- Prerequisites, limitations, and resources ................................................................................ 10
- Architecture overview ............................................................................................................. 11
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](https://aws.amazon.com/cloudformation/) 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/](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:

- [Using IAM Roles](https://docs.aws.amazon.com/IAM/latest/UserGuide/idRoleId.html)

**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, we strongly recommend 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, we strongly recommend a VPN connection to replicate data from an on-premises host to DDVE in the Cloud or vice versa.

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. We strongly recommend 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) and/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. Refer to 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 AZ's to provide Region redundancy using DD replication capabilities. The solution can also be deployed in alternative Regions to provide further redundancy as needed.

The following link provides more information:

- [DDVE in AWS Best Practices Guide](#)

---

**Getting Started**
CHAPTER 2

Introducing DDVE

This chapter includes the following topics:

- Introducing DDVE ................................................................. 14
- DDVE cloud features ........................................................... 14
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**

<table>
<thead>
<tr>
<th>Type</th>
<th>Resource configuration size</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDVE on Block storage</td>
<td>up to 16 TB</td>
</tr>
<tr>
<td>DDVE on S3 storage</td>
<td>up to 96 TB</td>
</tr>
</tbody>
</table>

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
• 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
• Bidirectional replication between on-premises and AWS
• DDVE supports a maximum of six active MTrees at a given time, however up to 100 MTrees can be created on the DDVE

The DD OS Administration Guide, DD Boost OST Guide, DD Boost for Partner Integration Administration Guide provide additional information about supported protocols and features.
Introducing DDVE
CHAPTER 3
Deploying DDVE

This chapter includes the following topics:

- Preparing your environment to deploy DDVE on AWS ............................................................. 18
- Deploying DDVE in AWS ........................................................................................................ 22
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.

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. Set up the network environment.
   For secure access to the DDVE, Dell EMC recommends that you use the VPC architecture provided by AWS. Set up and configure the following components:
   - VPC
   - Subnet
   - Route tables
   - Security groups
   - Network access control list
   - VPC Gateway endpoint for connectivity to S3

   Networking Best Practices for DDVE in the Cloud on page 63 provides more information.

2. Create an S3 bucket.

3. Set up 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 will be used in the IAM policy template to get access to the bucket and will also be used to create the object store profile on the DDVE.

Procedure

1. Login in to the AWS console. Select Services > S3.

2. Click Create bucket and enter the bucket name and region.

   ![Create S3 Bucket](image)

   - 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 S3 versioning for the bucket that is associated with the DDVE. 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**.

![Create bucket](image)

**Note:** Do not setup lifecycle rules for this bucket. Lifecycle 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. Create and attach the Identity and Access Management (IAM) role to DDVE to achieve access.

**Before you begin**

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

```
"iam:AddRoleToInstanceProfile",
"iam:AttachRolePolicy",
"iam:CreateRole",
"iam:DeleteRole",
"iam:DeleteRolePolicy",
```

Deploying DDVE
"iam:DetachRolePolicy",
"iam:GetRole",
"iam:GetRolePolicy",
"iam:ListRolePolicies",
"iam:GetRoles",
"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 access credentials are rotated periodically by the AWS infrastructure. The new credentials are automatically fetched by the DDVE just before the old credentials expire.

**Procedure**

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.
        ```json
        {
            "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. Please note that, in the resource tag below, use arn:aws-us-gov:s3:::my-bucket-name for AWS Gov clouds.
        ```json
        {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Action": [
                        "s3:ListBucket",
                        "s3:GetObject",
                        "s3:PutObject",
                        "s3:DeleteObject"
                    ],
                    "Resource": [
                        "arn:aws:s3:::my-bucket-name"
                    ]
                }
            ]
        }
        ```
d. Verify this information, and then click **Review policy**.

e. Provide a name and description for the policy.

```
arn:aws-us-gov:s3:::my-bucket-name,
arn:aws-us-gov:s3:::my-bucket-name/*
```

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:

      a. For **Select type of trusted entity**, select **AWS service**.

      b. 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 section. Select **Next Tags** to create a tag for the role.

   **Note:** Make a note of the policy name. It will be used to attach the policy to the role in the next step.
d. Click **Next: Review**. In the **Review** section, provide a name for the role and click **Create role**.

**After you finish**

You must attach the role to the DDVE instance before it can be configured. This 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 NVRAM and metadata disks in the correct order according to Storage best practices.

### Deploying DDVE using a Cloud Formation Template

This method is recommended.

**Procedure**

1. Go to the appropriate Website:
2. Search for PowerProtect DD Virtual.

3. Select Dell EMC PowerProtect DD Virtual Edition (DDVE) v4.0 and click Continue to Subscribe.

   ![Figure 3 Deploying DDVE using a CFT](image)

   **Note:** Your screen might be different than the one shown in the following figure.

4. Click Continue to Configuration.

   ![Figure 4 Subscribing to the software](image)

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 be deployed.
6. Review the configuration details, select Launch the Cloud Formation template, and then select Launch.
   The template URL is populated.

7. Click Next.

8. Enter the following values to create the stack.
   - Stack name
   - DDVE Capacity—Select any capacity from the drop down list. The recommended amount of metadata storage and the instance type for your selection is automatically attached by the template.
   - 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 Group ID
Note: The values in this figure are for illustration purposes. 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 that status of status of the stack you have created on the ddve-stack-test page.

12. When the stack creation is complete, navigate to the EC2 instances and select the region in which you have deployed the DDVE. Use the DDVE name tag from step 8 and verify that the corresponding EC2 instance is running.

Deploying DDVE manually from the AWS console

This is an alternate approach for deployment.

Procedure

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**.

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

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.
Note: It is important to add the NVRAM disk before adding the metadata disks. Adding them in a different order will result in an unsupported hardware configuration. Also, ensure that the EBS volume type is GP2.

### Table 3 Configuration

<table>
<thead>
<tr>
<th>Instance Type</th>
<th>Number of metadata disks</th>
<th>Size of each metadata disk</th>
<th>Object store capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>M4.xlarge</td>
<td>2</td>
<td>1024</td>
<td>16 TB</td>
</tr>
<tr>
<td>M4.2xlarge</td>
<td>4</td>
<td>1024</td>
<td>32 TB</td>
</tr>
<tr>
<td>M4.4xlarge</td>
<td>10</td>
<td>1024</td>
<td>96 TB</td>
</tr>
</tbody>
</table>

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.

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

   **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.

   ![Select an existing key pair or create a new key pair](image)

   **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**

   ![Select an existing key pair or create a new key pair](image)

   **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.**

   ![Select an existing key pair or create a new key pair](image)

   **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 backups have been initiated:
- Instance ID
- Instance Type
- Availability Zone
- Instance State
- Status Checks
- Alarms
- Public DNS (IPv4)

Get notified of estimated charges
Create alert rules 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 limit).

How to connect to your instances
Your instances are starting and will take a few minutes until they are in the running state, then 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 Instance to monitor your instance’s status. Once your instance is in the running state, you can access it from the instance page. Find out how to connect to your instances.

Here are some helpful resources to get you started:
- How to connect to your Linux instance
- Amazon EBS User Guide
- AWS Free Usage Tier
- Amazon EBS Discussion Forums
- Learn about AWS Free Usage Tier
- Amazon EBS User Guide

While your instances are launching you can also:
- Check instance launch status or 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

Open Instances

PowerProtect DD Virtual Edition on Amazon Web Services Installation and Administration Guide
CHAPTER 4

Completing Initial DDVE Configuration

This chapter includes the following topics:

- Configuring DDVE on AWS ................................................................. 32
- Recovering DDVE with system headswap .................................. 39
- Recovering the system ................................................................. 41
Configuring DDVE on AWS

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

**Before you begin**
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 32
- Using the CLI to configure the DDVE on page 35

**Using the DD System Manager to configure DDVE**

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

**Procedure**

1. Login 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
   - 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. At this point, 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.

Figure 7 Configure Storage

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.

Figure 8 File System complete

11. Click OK to proceed to the System Settings tab.

12. Change the DDVE password.
13. Configure the email server as required.

**Figure 10 Configure email server**

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

15. It is important for DDVE time to be synchronized with NTP for proper object store communication. Therefore, NTP must be configured for the DDVE that is running in AWS. To configure NTP server on the DDVE, do the following:

   a. Select **Administration > Settings**.
   
   b. Select **More Tasks > Configure Time Settings**.
   
   c. Under **More Tasks**, select **NTP > Manually Configure** and add the NTP servers as 0.amazon.pool.ntp.org.

**Figure 11 Configure NTP settings**

**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.

Procedure

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/password are supported.

Procedure

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
   
   $$\text{# ssh} \text{sysadmin@<IP address of DDVE>}
   
   EMC DD Virtual Edition
   
   Password:
   
   Welcome to DD OS 7.0.0.5-633941
   
   sysadmin@myddve0#$$

2. During the first login, users will be prompted to accept the EULA and change the password.
3. The configuration wizard will then be launched.
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. It will also will be used to encrypt keys if file system encryption is enabled.

• 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 DD OS 7.0.0.5-633941
-----------------------------------------
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:

<table>
<thead>
<tr>
<th>#</th>
<th>Feature</th>
<th>Capacity</th>
<th>Type</th>
<th>State</th>
<th>Expiration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CAPACITY</td>
<td>87.31 TiB</td>
<td>permanent (int)</td>
<td>active</td>
<td>n/a</td>
</tr>
</tbody>
</table>

** System is using internal licenses.

New Licenses:

<table>
<thead>
<tr>
<th>#</th>
<th>Feature</th>
<th>Capacity</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CAPACITY</td>
<td>87.31 TiB</td>
<td>permanent (int)</td>
</tr>
</tbody>
</table>

** 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]:

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

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

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

SMT Configuration
Configure SMT at this time (yes|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.

Config object store
DD VE is running in AWS. Role-based access will be used to access s3.
Enter the bucket name: sharms62-atos-bkt1
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.

Pending Object Store Settings
Bucket name: sharms62-atos-bkt1
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 attached to the DDVE:

```
# disk show hardware
```

<table>
<thead>
<tr>
<th>Disk</th>
<th>Slot</th>
<th>Manufacturer/Model</th>
<th>Firmware</th>
<th>Serial No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>----</td>
<td>--------------------</td>
<td>-----------</td>
<td>------------</td>
</tr>
<tr>
<td>dev1</td>
<td>-/a</td>
<td>Virtual BLOCK Device</td>
<td>n/a</td>
<td>(unknown) 250.0</td>
</tr>
<tr>
<td>dev2</td>
<td>-/b</td>
<td>Virtual BLOCK Device</td>
<td>n/a</td>
<td>(unknown) 10.0</td>
</tr>
<tr>
<td>dev3</td>
<td>-/c</td>
<td>Virtual BLOCK Device</td>
<td>n/a</td>
<td>(unknown) 1.0</td>
</tr>
</tbody>
</table>

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

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

7. Create and enable the file system:

```
# filesys create
# filesys enable
```

8. It is important that DDVE time is synchronized with NTP for proper object store communication. Therefore, NTP must be configured for the DDVE that is running in AWS. Run the following commands to configure NTP on the DDVE.

- `ntp add timeserver 0.amazon.pool.ntp.org`
- `ntp enable`
- `ntp sync`
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.

Procedure
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
2 -- -------- ------ --------------- ----- ----

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
5 -- ----------- ----- --------------- ----- ----

New licenses:
Capacity licenses:
## Feature Capacity Type State Expiration Date Note
-- -------- ------ --------------- ----- ----
1 CAPACITY 87.31 TiB permanent (int) active n/a
2 -- -------- ------ --------------- ----- ----

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. **New license(s) will overwrite all existing license(s).**
   Do you want to proceed? (yes|no) [yes]: yes
   eLicense(s) updated.

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

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

4. **Run the following command to create/modify the cloud profile:**

   ```
   # 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?
   (yes|no) [yes]: [yes]
   Profile is set
   ```

### Recovering DDVE with system headswap

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

**Before you begin**

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.

**Procedure**

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.

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.

6. Attach the metadata disks to instance B.

7. Set the system passphrase.

   ![Image](image_url)  

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

8. Attach the metadata disks to instance B.

9. Set the system passphrase.

   ![Image](image_url)  

   **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.

$ system headswap
This command returns the system back to its prior operational conditions. The system will be rebooted before resuming normal operations.

** Note: 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.

$ filesys 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.

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

```bash
# storage object-store enable
Object-store is enabled.
```
3. Set object-store profile:
   a. Set the passphrase to match system A, otherwise, the recovery will fail 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?
   (yes|no) [yes]: 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
   Object-store is not enabled. Filesystem will use block storage for user data.
   Do you want to continue? (yes|no) [no]: yes
   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. Execute 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 the filesys status after the recovery process completes:

   ```
   # filesys status
   The filesystem is enabled and running.
   ```
CHAPTER 5

Administering DDVE

This chapter includes the following topics:

- Adding virtual storage ................................................................. 44
- Extensions to DDOS for DDVE ..................................................... 44
- DDVE-only commands ................................................................. 45
- Modified DD OS commands ....................................................... 47
- Unsupported DD OS commands .................................................. 49
- Troubleshooting performance issues ........................................... 54
Adding virtual storage

Attach new metadata disks to the instance from the AWS console before adding them on the DDVE. Attaching an Amazon EBS Volume to an Instance provides additional information.

Additional virtual storage can be added to the DDVE using the GUI or the CLI.

Note: It is not possible to extend a virtual disk if it has already been used by the file system. Instead, expand the storage by adding a new virtual disk.

Using the GUI

In DD SM, click Hardware > Storage > Configure Storage to add the additional devices to the DDVE active tier.

Using the CLI

Run the storage add dev <n> command to add the disk to the DDVE.

When you add a new virtual data disk to an existing DDOS file system, use the filesys expand command instead of the filesys create command.

Configuring spindle groups

Do not manually configure any spindle groups. All spindle group configuration is done automatically.

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-regexp [module {default | ddfs}]
Disable tracing of specified events.

perf enable trace event-regexp [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-regexp [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]
```

```
sysadmin@zx-benmark-1# system vresource show requirements

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Tier</td>
<td>Cloud Tier</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Instance</td>
<td></td>
</tr>
<tr>
<td>Capacity (TB)</td>
<td>Capacity (TB)</td>
<td>Type</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>n/a</td>
<td>Standard_F4 (Only block storage is supported)</td>
</tr>
<tr>
<td>16</td>
<td>n/a</td>
<td>Standard_F8</td>
</tr>
<tr>
<td>32</td>
<td>n/a</td>
<td>Standard_D4_v2</td>
</tr>
<tr>
<td>96</td>
<td>n/a</td>
<td>Standard_D16_v3</td>
</tr>
<tr>
<td>256</td>
<td>n/a</td>
<td>Standard_D32s_v3</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The maximum allowed system capacity for active tier on block storage is 16 TB</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

DDVE-only commands

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

**Table 4 DDVE-only commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>elicense checkout feature-license &lt;feature-name-list&gt;</td>
<td>Allows user to check out the features of licenses for License Server installation</td>
</tr>
<tr>
<td>elicense checkout capacity-license &lt;feature-name&gt; value &lt;n&gt; {TB</td>
<td>GB}</td>
</tr>
<tr>
<td>sysadmin@localhost# elic checkout capacity-license value 10 TB</td>
<td>Checking out CAPACITY license will 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</td>
</tr>
<tr>
<td>sysadmin@localhost# elic checkout capacity-license value {TB</td>
<td>GB}</td>
</tr>
</tbody>
</table>
### Table 4 DDVE-only commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`elicense checkin {&lt;feature-name-list&gt;</td>
<td>all}`</td>
</tr>
<tr>
<td>`elicense license-server set server {&lt;ipaddr&gt;</td>
<td>&lt;hostname&gt;} port &lt;port-number&gt;`</td>
</tr>
<tr>
<td><code>elicense license-server reset</code></td>
<td>Returns DDVE to factory license settings.</td>
</tr>
<tr>
<td><code>elicense license-server show</code></td>
<td>Displays the usage for the metadata storage.</td>
</tr>
<tr>
<td><code>filesystems show space tier active local-metadata</code></td>
<td>Note: Some portion of the disk space is reserved for internal metadata, such as index. The amount of space is based on the maximum capacity of the platform and not on licensed capacity.</td>
</tr>
<tr>
<td><code>net hosts add</code></td>
<td>Two DDVEs in different regions cannot resolve each other’s hostname. Run this command to add a host list entry.</td>
</tr>
<tr>
<td><code>storage object-store enable</code></td>
<td>Enables the object-store feature for DDVE.</td>
</tr>
<tr>
<td><code>storage object-store disable</code></td>
<td>Disables the object-store feature for DDVE.</td>
</tr>
<tr>
<td><code>storage object-store profile set</code></td>
<td>Configures the object-store access profile.</td>
</tr>
<tr>
<td><code>storage object-store profile show</code></td>
<td>Displays the object-store access profile.</td>
</tr>
<tr>
<td><code>storage object-store profile status</code></td>
<td>This CLI lists the object-store profile information set on the DDVE.</td>
</tr>
<tr>
<td><code>system vresource show [requirements]</code></td>
<td>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 requirements option displays the physical storage requirements for DDVE.</td>
</tr>
<tr>
<td><code>vserver config set</code></td>
<td>DDVE supports the hypervisor’s functionality to collect performance statistics from the hypervisor. These performance statistics can be used to troubleshoot the DDVE performance problems. To do that, users need to specify the vServer information (hostname or IP address) and the credential information (username and password). The vServer can be a vCenter server, an ESXi host for vSphere, a Hyper-V server, or an SVCMM server for Hyper-V. Once this information is configured, DDVE will collect performance statistics from the vServer every 5 minutes.</td>
</tr>
</tbody>
</table>
### Table 4 DDVE-only commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vserver config reset</td>
<td>Reset the vServer credentials for DDVE to their default values.</td>
</tr>
<tr>
<td>vserver config show</td>
<td>Display the vServer credentials for DDVE.</td>
</tr>
</tbody>
</table>

### Modified DD OS commands

The behavior of the following commands has been modified on the DDVE platform:

### Table 5 Modified DD OS commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>alert</td>
<td>The tenant-unit parameter is not supported.</td>
</tr>
<tr>
<td>compression</td>
<td>The tenant-unit parameter is not supported.</td>
</tr>
<tr>
<td>config setup show</td>
<td>Arguments for configuring features not available in DDVE have been removed.</td>
</tr>
<tr>
<td>ddboost clients show active</td>
<td>The tenant-unit parameter is not supported.</td>
</tr>
<tr>
<td>ddboost file-replication show active</td>
<td>The tenant-unit parameter is not supported.</td>
</tr>
<tr>
<td>ddboost file-replication show detailed-file-history</td>
<td>The tenant-unit parameter is not supported.</td>
</tr>
<tr>
<td>ddboost file-replication show file-history</td>
<td>The tenant-unit parameter is not supported.</td>
</tr>
<tr>
<td>ddboost option reset</td>
<td>The fc parameter is not supported.</td>
</tr>
<tr>
<td>ddboost option show</td>
<td>The fc parameter is not supported.</td>
</tr>
<tr>
<td>ddboost storage-unit create</td>
<td>The tenant-unit parameter is not supported.</td>
</tr>
<tr>
<td>ddboost storage-unit modify</td>
<td>The tenant-unit parameter is not supported.</td>
</tr>
<tr>
<td>ddboost storage-unit show</td>
<td>The tenant-unit parameter is not supported.</td>
</tr>
<tr>
<td>ddboost streams show active</td>
<td>The tenant-unit parameter is not supported.</td>
</tr>
<tr>
<td>ddboost streams show history</td>
<td>The tenant-unit parameter is not supported.</td>
</tr>
<tr>
<td>disk rescan</td>
<td>The &lt;enlcosure-ID&gt;.&lt;disk-ID&gt; parameter is not supported.</td>
</tr>
</tbody>
</table>
### Table 5 Modified DD OS commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>disk show state</td>
<td>DDVE system disks show the System Dev state.</td>
</tr>
<tr>
<td>disk show stats</td>
<td>The DDVE format for this command is <code>disk show stats [dev &lt;n&gt;]</code></td>
</tr>
<tr>
<td>disk status</td>
<td>The Spare row has been removed from the output. The System row has been added.</td>
</tr>
<tr>
<td>enclosure show all</td>
<td>The <code> [&lt;enclosure&gt;]</code> parameter is not supported.</td>
</tr>
<tr>
<td>enclosure show controllers</td>
<td>The <code> [&lt;enclosure&gt;]</code> parameter is not supported.</td>
</tr>
<tr>
<td>enclosure show cpus</td>
<td>The <code> [&lt;enclosure&gt;]</code> parameter is not supported.</td>
</tr>
<tr>
<td>enclosure show io-cards</td>
<td>The <code> [&lt;enclosure&gt;]</code> parameter is not supported.</td>
</tr>
<tr>
<td>enclosure show memory</td>
<td>The <code> [&lt;enclosure&gt;]</code> parameter is not supported.</td>
</tr>
<tr>
<td>filesystem encryption keyes delete</td>
<td>The ` [tier {active</td>
</tr>
<tr>
<td>filesystem encryption keys show</td>
<td>The ` [tier {active</td>
</tr>
<tr>
<td>filesystem fastcopy</td>
<td>The <code> [retention-lock]</code> parameter is supported with DDVE 4.0. Retention lock governance mode is supported for DDVE on premises. Retention lock compliance mode is not supported for any DDVE.</td>
</tr>
<tr>
<td>filesystem show compression</td>
<td>The ` [tier {active</td>
</tr>
<tr>
<td>filesystem show space</td>
<td>The ` [tier {active</td>
</tr>
<tr>
<td>mtree create</td>
<td>The tenant-unit parameter is not supported.</td>
</tr>
<tr>
<td>mtree list</td>
<td>The tenant-unit parameter is not supported.</td>
</tr>
<tr>
<td>mtree show compression</td>
<td>The tenant-unit parameters are not supported.</td>
</tr>
</tbody>
</table>
### Table 5 Modified DD OS commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>mtree show performance</td>
<td>The <code>tenant-unit</code> parameter is not supported.</td>
</tr>
<tr>
<td>net create interface</td>
<td>The <code>&lt;virtual-ifname&gt;</code> parameter is not supported.</td>
</tr>
<tr>
<td>net destroy</td>
<td>The <code>&lt;virtual-ifname&gt;</code> parameter is not supported.</td>
</tr>
<tr>
<td>perf</td>
<td>The <code>vtl</code> option is not supported on any <code>perf</code> command.</td>
</tr>
<tr>
<td>storage add</td>
<td>The <code>enclosure</code> and <code>disk</code> parameters are not supported.</td>
</tr>
<tr>
<td>storage remove</td>
<td>The <code>enclosure</code> and <code>disk</code> parameters are not supported.</td>
</tr>
<tr>
<td>storage show</td>
<td>The <code>archive</code> option is not supported.</td>
</tr>
<tr>
<td>system show stats</td>
<td>NVRAM statistics are not reported, because DDVE systems do not have physical NVRAM.</td>
</tr>
<tr>
<td>quota</td>
<td>The <code>tenant-unit</code> parameter is not supported.</td>
</tr>
<tr>
<td>replication</td>
<td>MTree replication is the only type of replication supported.</td>
</tr>
<tr>
<td>snapshot</td>
<td>The <code>tenant-unit</code> parameter is not supported.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Unsupported command or command option</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>adminaccess https generate certificate</td>
<td>Deprecated. Use <code>adminaccess certificate generate</code> instead.</td>
</tr>
<tr>
<td>alerts add</td>
<td>Deprecated. Use <code>alerts notify-list add</code> instead.</td>
</tr>
<tr>
<td>alerts del</td>
<td>Deprecated. Use <code>alerts notify-list del</code> instead.</td>
</tr>
<tr>
<td>alerts notify-list option set group-name tenant-alert-summary {enabled</td>
<td>disabled}</td>
</tr>
<tr>
<td>alerts notify-list option reset group-name tenant-alert-summary</td>
<td></td>
</tr>
<tr>
<td>alerts reset</td>
<td>Deprecated. Use <code>alerts notify-list reset</code> instead.</td>
</tr>
<tr>
<td>Unsupported command or command option</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>alerts show alerts-list</td>
<td>Deprecated. Use alerts notify-list show instead.</td>
</tr>
<tr>
<td>alerts test</td>
<td>Deprecated. Use alerts notify-list test instead.</td>
</tr>
<tr>
<td>archive</td>
<td></td>
</tr>
<tr>
<td>authorization</td>
<td></td>
</tr>
<tr>
<td>autosupport display</td>
<td>Deprecated. Use autosupport show report instead.</td>
</tr>
<tr>
<td>autosupport reset support-list</td>
<td>Deprecated. Use autosupport reset { all</td>
</tr>
<tr>
<td>autosupport show support-list</td>
<td>Deprecated. Use autosupport show { all</td>
</tr>
<tr>
<td>cifs set authentication nt4</td>
<td>Deprecated. Use cifs set authentication active-directory instead.</td>
</tr>
<tr>
<td>cluster</td>
<td></td>
</tr>
<tr>
<td>ddboost fc</td>
<td></td>
</tr>
<tr>
<td>ddboost option reset fc</td>
<td></td>
</tr>
<tr>
<td>ddboost option set distributed-segment-processing disabled</td>
<td>Turning off distributed segment processing (DSP) with this DDBoost command is not supported for DDVE on DD OS 6.1.2.x.</td>
</tr>
<tr>
<td>ddboost option show</td>
<td>Turning off DSP with this DDBoost command is not supported for DDVE on DD OS 6.1.2.x.</td>
</tr>
<tr>
<td>ddboost option show fc</td>
<td></td>
</tr>
<tr>
<td>ddboost show image-duplication</td>
<td>Deprecated. Use ddboost file-replication show instead.</td>
</tr>
<tr>
<td>ddboost user option set user default-tenant-unit tenant-unit</td>
<td></td>
</tr>
<tr>
<td>ddboost user option reset user [default-tenant-unit]</td>
<td></td>
</tr>
<tr>
<td>disk add dev disk-id [spindle-group 1-16]</td>
<td>Deprecated. Use storage add instead.</td>
</tr>
<tr>
<td>disk add enclosure enclosure-id</td>
<td>Deprecated. Use storage add instead.</td>
</tr>
<tr>
<td>disk benchmark start</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>disk benchmark show</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>disk benchmark stop</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>disk benchmark watch</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>disk expand</td>
<td>Deprecated. Use storage add instead.</td>
</tr>
<tr>
<td>disk failenclosure-id disk-id</td>
<td></td>
</tr>
<tr>
<td>disk multipath</td>
<td></td>
</tr>
<tr>
<td>Unsupported command or command option</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>disk port</td>
<td></td>
</tr>
<tr>
<td>disk rescan [enclosure-id.disk-id]</td>
<td></td>
</tr>
<tr>
<td>disk show detailed-raid-info</td>
<td>Deprecated. Use disk show state and storage show instead.</td>
</tr>
<tr>
<td>disk show failure-history</td>
<td></td>
</tr>
<tr>
<td>disk show performance</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>disk show raid-info</td>
<td>Deprecated. Use disk show state and storage show instead.</td>
</tr>
<tr>
<td>disk show reliability-data</td>
<td></td>
</tr>
<tr>
<td>disk disk show stats</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>disk unfail</td>
<td></td>
</tr>
<tr>
<td>enclosure beacon</td>
<td></td>
</tr>
<tr>
<td>enclosure show all [enclosure]</td>
<td>This command is supported, but not with the enclosure argument.</td>
</tr>
<tr>
<td>enclosure show chassis</td>
<td></td>
</tr>
<tr>
<td>enclosure show controllers enclosure</td>
<td>This command is supported, but not with the enclosure argument.</td>
</tr>
<tr>
<td>enclosure show cpus [enclosure]</td>
<td>This command is supported, but not with the enclosure argument.</td>
</tr>
<tr>
<td>enclosure show fans</td>
<td></td>
</tr>
<tr>
<td>enclosure show io-cards [enclosure]</td>
<td>This command is supported, but not with the enclosure argument.</td>
</tr>
<tr>
<td>enclosure show memory [enclosure]</td>
<td>This command is supported, but not with the enclosure argument.</td>
</tr>
<tr>
<td>enclosure show nvramp</td>
<td></td>
</tr>
<tr>
<td>enclosure show powersupply</td>
<td></td>
</tr>
<tr>
<td>enclosure show summary</td>
<td></td>
</tr>
<tr>
<td>enclosure show temperature-sensors</td>
<td></td>
</tr>
<tr>
<td>enclosure show topology</td>
<td></td>
</tr>
<tr>
<td>enclosure test topology</td>
<td></td>
</tr>
<tr>
<td>filesystems archive</td>
<td></td>
</tr>
<tr>
<td>filesystems clean update-stats</td>
<td>Deprecated. Use filesystems show space instead.</td>
</tr>
<tr>
<td>filesystems encryption</td>
<td></td>
</tr>
<tr>
<td>filesystems encryption passphrase change</td>
<td>Deprecated. Use system passphrase change instead.</td>
</tr>
<tr>
<td>filesystems retention-lock</td>
<td>Deprecated. Use mtree retention-lock instead.</td>
</tr>
</tbody>
</table>
Table 6 Unsupported commands and command options (continued)

<table>
<thead>
<tr>
<th>Unsupported command or command option</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>filesys show compression tier</td>
<td>The tier option is not supported.</td>
</tr>
<tr>
<td>filesys show history</td>
<td>Deprecated. Use filesys show compression daily instead.</td>
</tr>
<tr>
<td>ha create</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>ha destroy</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>ha status</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>ha failover</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>ha online</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>ha offline</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>license</td>
<td>The license commands are not supported because DDVE uses new elicense commands.</td>
</tr>
<tr>
<td>mtree show compression mtree_path tier</td>
<td></td>
</tr>
<tr>
<td>net aggregate</td>
<td></td>
</tr>
<tr>
<td>net config ifname type cluster</td>
<td></td>
</tr>
<tr>
<td>net create interface virtual-ifname</td>
<td></td>
</tr>
<tr>
<td>net create interface physical-ifname vlan</td>
<td></td>
</tr>
<tr>
<td>net create virtual vethid</td>
<td></td>
</tr>
<tr>
<td>net destroy virtual-ifname</td>
<td></td>
</tr>
<tr>
<td>net destroy vlan-ifname</td>
<td></td>
</tr>
<tr>
<td>net failover</td>
<td></td>
</tr>
<tr>
<td>net modify virtual-ifname bonding</td>
<td></td>
</tr>
<tr>
<td>net modify virtual-ifname bonding</td>
<td>aggregate</td>
</tr>
<tr>
<td>net set portnaming</td>
<td></td>
</tr>
<tr>
<td>ndmp</td>
<td></td>
</tr>
<tr>
<td>ndmpd</td>
<td></td>
</tr>
<tr>
<td>nfs option enable report-replica-as writable</td>
<td>Deprecated. Use filesys option enable report-replica-as-writable instead.</td>
</tr>
<tr>
<td>nfs option show report-replica-as writable</td>
<td>Deprecated. Use filesys option show report-replica-as-writable instead.</td>
</tr>
<tr>
<td>perf * module vtl</td>
<td></td>
</tr>
<tr>
<td>Unsupported command or command option</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>san</td>
<td></td>
</tr>
<tr>
<td>shelf migration start</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>shelf migration status</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>shelf migration suspend</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>shelf migration resume</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>shelf migration precheck</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>shelf migration finalize</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>shelf migration show history</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>snapshot add schedule name [days days]</td>
<td>time time [,time...] [retention period]</td>
</tr>
<tr>
<td>snapshot del schedule {name</td>
<td>all}</td>
</tr>
<tr>
<td>snapshot modify schedule name {[days days]</td>
<td>time time [,time...]</td>
</tr>
<tr>
<td>snapshot reset schedule</td>
<td>Deprecated. Use snapshot schedule reset instead.</td>
</tr>
<tr>
<td>snapshot show schedule</td>
<td>Deprecated. Use snapshot schedule show instead.</td>
</tr>
<tr>
<td>storage add enclosure enclosure-id</td>
<td></td>
</tr>
<tr>
<td>storage add disk enclosure-id.disk-id</td>
<td></td>
</tr>
<tr>
<td>storage remove enclosure enclosure-id</td>
<td></td>
</tr>
<tr>
<td>storage remove disk enclosure_id.disk-id</td>
<td></td>
</tr>
<tr>
<td>system firmware</td>
<td></td>
</tr>
<tr>
<td>system option set console</td>
<td></td>
</tr>
<tr>
<td>system retention-lock</td>
<td></td>
</tr>
<tr>
<td>system sanitize</td>
<td></td>
</tr>
<tr>
<td>Unsupported command or command option</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>system show anaconda</td>
<td></td>
</tr>
<tr>
<td>system show controller-inventory</td>
<td></td>
</tr>
<tr>
<td>system show nvram</td>
<td></td>
</tr>
<tr>
<td>system show nvram-detailed</td>
<td></td>
</tr>
<tr>
<td>system show oemid</td>
<td></td>
</tr>
<tr>
<td>system upgrade continue</td>
<td></td>
</tr>
<tr>
<td>user</td>
<td></td>
</tr>
<tr>
<td>user change priv</td>
<td>Deprecated, with no replacement.</td>
</tr>
<tr>
<td>vserver config set host</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>vserver config reset</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>vserver config show</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>vserver config perf-stats start</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>vserver config perf-stats stop</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>vserver config perf-stats status</td>
<td>Not supported by DDVE in cloud</td>
</tr>
<tr>
<td>vtl lunmask</td>
<td>Deprecated. Use vtl group instead.</td>
</tr>
<tr>
<td>vtl lunmask add</td>
<td>Deprecated. Use vtl group add instead.</td>
</tr>
<tr>
<td>vtl lunmask del</td>
<td>Deprecated.</td>
</tr>
<tr>
<td>vtl lunmask show</td>
<td>Deprecated. Use vtl group show instead.</td>
</tr>
</tbody>
</table>

**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 44 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.
This chapter includes the following topics:

- ASUP configuration .......................................................... 58
- AWS licensing ................................................................. 58
- Storage best practices ....................................................... 58
- Security best practices ..................................................... 60
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 server 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 instance types and storage types required for object storage.

<table>
<thead>
<tr>
<th>DDVE configuration</th>
<th>Instance type</th>
<th>Storage configuration type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Root disk</td>
</tr>
<tr>
<td>Up to 16 TB</td>
<td>M4.xlarge</td>
<td>250 GB</td>
</tr>
</tbody>
</table>
Table 7 Storage size specifications (continued)

<table>
<thead>
<tr>
<th>DDVE configuration</th>
<th>Instance type</th>
<th>Root disk</th>
<th>NVRAM disk</th>
<th>Metadata disk</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 to 32 TB</td>
<td>M4.2xlarge</td>
<td>250 GB</td>
<td>10 GB</td>
<td>4 x 1024 GB</td>
</tr>
<tr>
<td>32 to 96 TB</td>
<td>M4.4xlarge</td>
<td>250 GB</td>
<td>10 GB</td>
<td>10 x 1024 GB</td>
</tr>
</tbody>
</table>

**Note:**
- If the incorrect storage type is used, the system displays an alert for an unsupported virtual hardware configuration.
- The metadata requirements listed for above are based on a 10 x deduplication ratio and a 2 x compression ratio. Some configurations may require a higher storage ratio. If the system displays an alert that additional storage is required, expand the storage.

**Block storage specifications**

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

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

<table>
<thead>
<tr>
<th>DDVE configuration</th>
<th>Instance type</th>
<th>Root disk type/size</th>
<th>NVRAM disk type/size</th>
<th>Data disk type/size</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 TB</td>
<td>M4.xlarge</td>
<td>GP2/250 GB</td>
<td>GP2/10 GB</td>
<td>GP2/1024 GB</td>
</tr>
</tbody>
</table>

**Note:**
- DDVE with block storage supports a maximum capacity of 16 TB.
- If the incorrect storage type is used, the system displays an alert for an incorrect virtual hardware configuration.

Table 9 AWS stream counts

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Memory</th>
<th>Number of 1 TiB metadata disks</th>
<th>Stream counts</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Read</td>
<td>Write</td>
<td>Replication in</td>
<td>Replication out</td>
</tr>
<tr>
<td>16 TB (M4.xlarge)</td>
<td>16 GB</td>
<td>1</td>
<td>12</td>
<td>36</td>
<td>36</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>24</td>
<td>36</td>
<td>36</td>
<td>36</td>
</tr>
<tr>
<td>32 TB (M4.2xlarge)</td>
<td>32 GB</td>
<td>1</td>
<td>12</td>
<td>48</td>
<td>48</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>24</td>
<td>72</td>
<td>72</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 or more</td>
<td>40</td>
<td>72</td>
<td>72</td>
<td>48</td>
</tr>
<tr>
<td>96 TB (M4.4xlarge)</td>
<td>64 GB</td>
<td>1</td>
<td>12</td>
<td>48</td>
<td>48</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>24</td>
<td>96</td>
<td>96</td>
<td>48</td>
</tr>
</tbody>
</table>
Table 9 AWS stream counts (continued)

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Memory</th>
<th>Number of 1 TiB metadata disks</th>
<th>Stream counts</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Read</td>
</tr>
<tr>
<td></td>
<td>3 or more</td>
<td></td>
<td>40</td>
</tr>
</tbody>
</table>

Note: The metadata requirements listed for supported virtualization platforms are based on a 10x deduplication ratio and a 2x compression ratio. Some configurations may require a higher storage ratio. Expand the storage if the system displays an alert that additional storage is required.

Metadata disk storage expansion notes

Metadata disks can be added incrementally in 1 TiB increments. Add additional metadata disks as required to reach the recommended number of metadata disks for the instance type. The number of metadata disks by instance is based on the assumption of a 2x overall deduplication ratio (10x deduplication and 2x compression). For workloads with higher deduplication ratios, additional metadata storage is required.

Table 10 Recommended metadata disks by instance

<table>
<thead>
<tr>
<th>Instance type</th>
<th>Recommended number of metadata disks</th>
</tr>
</thead>
<tbody>
<tr>
<td>M4.xlarge</td>
<td>2</td>
</tr>
<tr>
<td>M4.2xlarge</td>
<td>4</td>
</tr>
<tr>
<td>M4.4xlarge</td>
<td>10</td>
</tr>
</tbody>
</table>

Spindle group

There is no need 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 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 will fail.
- 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 have been removed by the GC cycle(s).
- Do not configure any life cycle policy on the bucket as it might result in loss of critical data.

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.

---

PowerProtect DD Virtual Edition on Amazon Web Services Installation and Administration Guide
### Table 11 Access Types and Authentication

<table>
<thead>
<tr>
<th>Access Type</th>
<th>Authentication Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUI</td>
<td>username/password, X509 certificates</td>
</tr>
<tr>
<td>SSH</td>
<td>username/password, SSH key pair</td>
</tr>
<tr>
<td>REST API</td>
<td>username/password, X509 certificates</td>
</tr>
</tbody>
</table>

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 12 Inbound ports used by DDVE

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 22</td>
<td>SSH</td>
<td>Used for SSH (CLI) access and for configuring DDVE.</td>
</tr>
<tr>
<td>TCP 443</td>
<td>HTTPS</td>
<td>Used for DDSM (GUI) access and for configuring DDVE.</td>
</tr>
</tbody>
</table>
Table 12 Inbound ports used by DDVE (continued)

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 2049</td>
<td>DD Boost/NFS</td>
<td>Main port used by NFS - can be modified using the <code>nfs set server-port</code> command which requires SE mode.</td>
</tr>
<tr>
<td>TCP 2051</td>
<td>Replication/DD Boost/ Optimized Duplication</td>
<td>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>.</td>
</tr>
<tr>
<td>TCP 3009</td>
<td>SMS (system management)</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 13 Outboard ports used by DDVE

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP 123</td>
<td>NTP</td>
<td>Used by the DD system to synchronize to a time server.</td>
</tr>
<tr>
<td>TCP 443</td>
<td>HTTPS</td>
<td>Used for DDVE to be able to communicate with outside services.</td>
</tr>
<tr>
<td>TCP 2049</td>
<td>DD Boost/NFS</td>
<td>Main port used by NFS - can be modified using the <code>nfs set server-port</code> command which requires SE mode.</td>
</tr>
<tr>
<td>TCP 2051</td>
<td>Replication/DD Boost/ Optimized Duplication</td>
<td>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>.</td>
</tr>
<tr>
<td>TCP 2051</td>
<td>SMS (system management)</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

Networking Best Practices for DDVE in the Cloud

This chapter includes the following topics:

- Network setup in AWS .............................................................. 64
- Network infrastructure setup ...................................................... 65
- Setting up NTP time synchronization in AWS .............................. 66
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 14 DDVE Inbound Ports**

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 22</td>
<td>SSH</td>
<td>Used for SSH (CLI) access and for configuring DDVE.</td>
</tr>
<tr>
<td>TCP 443</td>
<td>HTTPS</td>
<td>Used for DDSM (GUI) access and for configuring DDVE.</td>
</tr>
<tr>
<td>TCP 2049</td>
<td>DD Boost/NFS</td>
<td>Main port used by NFS - can be modified using the <code>nfs set server-port</code> command which requires SE mode.</td>
</tr>
<tr>
<td>TCP 2051</td>
<td>Replication/DD Boost/ Optimized Duplication</td>
<td>Used only if replication is configured (run <code>replication show config on DD system to determine</code>). This port can be modified using <code>replication modify</code>.</td>
</tr>
<tr>
<td>TCP 3009</td>
<td>SMS (system management)</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 15 DDVE Outbound Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP 123</td>
<td>NTP</td>
<td>Used by the DD system to synchronize to a time server.</td>
</tr>
<tr>
<td>TCP 443</td>
<td>HTTPS</td>
<td>Used for DDVE to be able to communicate with Object store (S3).</td>
</tr>
<tr>
<td>TCP 2049</td>
<td>DD Boost/NFS</td>
<td>Main port used by NFS - can be modified using the <code>nfs set server-port</code> command which requires SE mode.</td>
</tr>
<tr>
<td>TCP 2051</td>
<td>Replication/DD Boost/ Optimized Duplication</td>
<td>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>.</td>
</tr>
<tr>
<td>TCP 3009</td>
<td>SMS (system management)</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

**Setting up NTP time synchronization in AWS**

Configure NTP on the DDVE instance that runs in AWS.

**About this task**

A drift in time can impact the object store communication, because system time is required for secure communication. When you perform the initial configuration of the DDVE system, enable NTP and configure the NTP server.

You can use the DD System Manager, the CLI configuration wizard, or the `ntp enable` command on the DD OS command line.

To configure NTP on the DDVE instance using CLI, run the following commands:

- `ntp add timeserver 0.amazon.pool.ntp.org`
- `ntp enable`
- `ntp sync`

If your system does not have an NTP server, Amazon recommends that you use the following command to configure NTP:

```
server 0.amazon.pool.ntp.org
```

AWS documentation provides more information.

The following procedure uses DD System Manager to configure NTP on the DDVE instance.

**Procedure**

1. Select Administration > Settings > More Tasks > Configure Time Settings
2. Under NTP, select Manually Configure and add the NTP servers as 0.amazon.pool.ntp.org.
APPENDIX C

Installing and Configuring DDVE on Block Storage in the Cloud

This chapter includes the following topics:

- Overview of DDVE on block storage .............................................................. 68
- Configuring DDVE on block storage with DD System Manager .................... 68
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.

Procedure

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.