

Dell EMC PowerProtect DD Management Center

Installation and Administration Guide

7.3

Notes, cautions, and warnings

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

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

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

Revision history.....	7
Chapter 1: PowerProtect DDMC Overview.....	8
Introducing PowerProtect DDMC.....	8
Features and limitations of DDMC.....	8
Differences between DDMC and DD System Manager.....	9
Chapter 2: Planning the DDMC environment.....	10
System requirements.....	10
Determining VMware requirements.....	10
VMware hardware and software system requirements.....	10
Additional VMware software applications.....	11
Backing up and restoring.....	11
Chapter 3: Getting Started.....	12
Prerequisites.....	12
Downloading DDMC.....	12
Installing DDMC in a VMware environment.....	13
Installing on a VMware vCenter Server.....	14
Installing on a VMware ESX server.....	15
Hyper-V.....	15
DDMC on kernel-based virtual machine.....	16
Manageability in public cloud.....	18
Powering on DDMC.....	25
Logging in and out of DDMC.....	25
Logging into DDMC.....	26
Logging in with Public Key Infrastructure (PKI) and Common Access Card (CAC) certificates.....	26
Logging out of DDMC.....	27
Continuing DDMC configuration.....	27
Understanding RBAC in DDMC.....	27
Viewing DDMC page elements.....	27
Navigating a DDMC page.....	28
Organizing the dashboard.....	28
Adding and configuring tabs.....	28
Adding widgets.....	29
Copying tabs.....	31
Filtering tabs.....	32
Modifying widgets.....	32
Organizing managed Data Domain or PowerProtect systems.....	32
Creating groups.....	32
Adding properties to systems and replication pairs.....	33
Adding (registering) systems to DDMC.....	33
Configuration Templates.....	34
Inbound and outbound proxy host names and port numbers used by the firewall.....	35
Editing Data Domain or PowerProtect system settings.....	37

Assigning properties.....	38
Assigning system property values.....	38
Assigning replication property values.....	38
Displaying property information.....	39
Displaying properties for an element.....	39
Finding elements by property value.....	39
Managing groups.....	40
Managing replication lag threshold policies.....	40
Working with filters.....	41
Chapter 4: Monitoring Systems.....	42
How DDMC helps you monitor Data Domain and PowerProtect systems.....	42
Data retention policy for DDMC.....	42
Space projection algorithm for DDMC.....	43
Performing daily monitoring.....	43
Checking dashboard status widgets.....	43
Checking alert notifications.....	45
Checking health status.....	45
Checking health alerts.....	46
Checking health jobs.....	46
Monitoring capacity.....	47
Checking system capacity and disk space usage.....	47
Measuring physical capacity.....	48
Checking projected system capacity.....	51
Interacting with the Projection Chart.....	52
Checking the System Details lightbox.....	52
Monitoring replication.....	53
Viewing replication topology to investigate error conditions.....	55
Checking the Replication Pair Details lightbox.....	55
Monitoring status with reports.....	56
Creating a report with the wizard.....	56
Generating a report immediately.....	57
Cleaning up reports from deleted users.....	57
Chapter 5: Managing Data Domain and PowerProtect Systems.....	58
Launching DD System Manager.....	58
Upgrading system software.....	58
Managing system upgrade packages.....	59
Performing a system upgrade.....	59
Local users.....	60
Creating access for users.....	60
Chapter 6: Administering Secure Multi-Tenancy.....	62
How DDMC helps with SMT monitoring.....	62
Secure Multi-Tenancy overview.....	62
Managing Tenant users and their privileges	67
Using DDMC to administer SMT.....	67
Creating and managing Tenants.....	68
Creating Tenants.....	68

Viewing Tenant information and status.....	69
Tenant Details lightbox.....	69
Editing Tenant information.....	70
Deleting Tenants.....	70
Creating and managing Tenant Units.....	71
Creating a Tenant Unit with the wizard.....	71
Viewing Tenant Unit information and status.....	73
Tenant Unit Details lightbox.....	73
Editing Tenant Unit information.....	74
Deleting Tenant Units and unassigning provisioned storage.....	78
Adding an unmanaged Tenant Unit to a Tenant.....	79
Creating, editing, and generating SMT reports.....	79
SMT report permission table.....	79
Creating SMT report templates.....	80
Editing SMT report templates.....	81
Generating SMT reports.....	81
Chapter 7: Performing Additional Configuration.....	83
Managing network settings.....	83
Configuring network settings.....	83
Configuring network interfaces.....	84
Configuring hosts.....	85
Configuring DNS settings.....	87
Configuring routes.....	88
Working with SNMP.....	91
Managing access to DD Management Center.....	98
Roles required for DDMC tasks.....	98
Managing administrator access.....	100
Managing local user access to DDMC.....	103
Active users.....	109
Configuring authentication.....	110
Managing general configuration settings.....	116
Configuring time and date settings.....	116
Configuring system properties.....	117
Managing alerts.....	118
Managing autosupport reporting.....	120
Managing system logs.....	121
Upgrading DDMC software.....	121
Appendix A: Graphics Reference for DDMC.....	123
Global controls and icons.....	123
Dashboard controls.....	125
Widget controls.....	125
Group icons.....	126
Property controls.....	126
Appendix B: Command Line Interface for DDMC.....	128
Differences between DDMC CLI and DD OS CLI.....	128
Tasks available only in DDMC CLI.....	128

config template commands.....	128
config template apply.....	128
config template create.....	129
config template creation schedule set.....	130
config template creation schedule reset.....	130
config template destroy.....	130
config template rename.....	130
config template show detailed.....	130
config template show list.....	130
managed-system commands.....	131
managed-system add.....	131
managed-system check-connection.....	131
managed-system delete.....	132
managed-system resume.....	132
managed-system set.....	132
managed-system show.....	132
managed-system suspend.....	133
managed-system sync.....	134
task commands.....	134
task cancel.....	134
task pause.....	134
task resume.....	134
task show active.....	134
task show detailed.....	135
task show detailed-active.....	135
task show detailed-history.....	135
task show history.....	136

Revision history

The following table presents the revision history of this document.

Table 1. Document revision history

Revision	Date	Description
01	August 2020	Initial publication

PowerProtect DDMC Overview

Topics:

- [Introducing PowerProtect DDMC](#)
- [Features and limitations of DDMC](#)
- [Differences between DDMC and DD System Manager](#)

Introducing PowerProtect DDMC

DDMC is a scalable, virtual system-based solution for centralized management of multiple Data Domain or PowerProtect systems and virtual data protection systems (DDVE instances).

- DDMC provides current and historical data for all of the managed systems, with subject presentation ranging from site-wide summaries to granular detail for a selected object.
- DDMC can monitor storage on multiple systems with Secure Multi-tenancy, DD Boost backup, and replication.
- DDMC is composed of browser-based pages and is installed and runs on a VMware, Hyper-V, KVM, or public cloud environment (for example, Amazon Web Services (AWS), Azure, or Google Cloud Platform (GCP)).

 **NOTE:** Secure Multi-tenancy is only supported on DDVE 3.0 and later.

Features and limitations of DDMC

The robust features of DDMC help manage all of the Data Domain or PowerProtect systems through one convenient user interface.

These features enable you to:

- Monitor and manage
 - Monitor the health and operation of managed objects on a user-configurable dashboard
 - Display site-wide storage capacity, showing aggregated usage totals, including Cloud Tier
 - Graph current and historical data about space usage, data consumption, and daily written data trends
 - Manage the Secure MultiTenancy (SMT) feature, especially to configure and monitor DD Boost access
 - Monitor operational status of configured replications and set thresholds that generate alerts (sent to the alerts log) when replications lag
 - Manage user access through configurable role-based access control (RBAC) settings
- Estimate and report
 - Estimate projected capacity needs based on historical trends and pinpoint specific dates (both past and future) for usage comparison
 - Generate usage and performance reports, on demand, or set up a schedule and email list to facilitate proactive management
 - Process alerts for all managed Data Domain or PowerProtect systems, including Cloud Tier, and view from a single list
 - Secure Remote Service V3 gateway (GW) integration provides secure transport of messages to Dell support
- Act simultaneously on multiple Data Domain or PowerProtect systems
 - Multiple-system management capabilities with DDMC and full single-system management capabilities with DD System Manager
 - Create custom groupings of the managed Data Domain or PowerProtect systems, organized efficiently and intentionally
 - Apply groups and properties to managed objects to customize how content is displayed and best represent the infrastructure
 - Configure Secure MultiTenancy tenants and tenant units for the managed Data Domain or PowerProtect systems individually, or in groups, such as user access and DD OS upgrades

DDMC can be deployed on Hyper-V platforms and in public cloud environments (for example, AWS, Azure, and Google Cloud Platform).

Unsupported protocols and features

The following protocols and features are not supported in DDMC and should be considered as product limitations:

- No backup in DDMC
- No file system
- DD Boost
- Replicator software
- DD Encryption
- NFS
- Kerberos authentication

DD OS commands related to these unsupported features are not supported in DDMC.

Differences between DDMC and DD System Manager

DDMC differs from DD System Manager in the following ways:

- DDMC can manage up to 150 Data Domain or PowerProtect systems, while DD System Manager is a single-system management tool.
 - DDMC includes the ability to manage systems with High Availability (HA), Cloud Tier, and DDVE instances.
- DDMC can perform upgrade on groups of Data Domain or PowerProtect systems simultaneously.
- DDMC aggregates storage and performance data and compares operational information for all managed systems. DD System Manager does not aggregate storage or performance data from multiple systems, nor can you compare operational information across systems.
- DDMC does not directly manage storage. DDSM directly manages storage (using VTL, CIFS, NFS, DD Boost, and so on).
- DDMC cannot configure and manage any replication or encryption.

Planning the DDMC environment

Topics:

- [System requirements](#)
- [Determining VMware requirements](#)
- [Backing up and restoring](#)

System requirements

The virtual machine hardware requirements are provided in this table.

Table 2. System requirements

# of systems managed	virtual CPU (vCPU)	memory (GB)	VM disk SizeBase install + database (GB)
1 to 150	4 vCPU	8	40 + 200

NOTE: The changing of any of the individual components of these settings is not supported, that is, you cannot increase the memory, change the CPU settings, etc.

Determining VMware requirements

VMware requirements include:

- [VMware hardware and software system requirements](#) on page 10
- [Additional VMware software applications](#) on page 11

VMware hardware and software system requirements

The VMware hardware and software that is required to host a DDMC installation can be:

- The vCenter Server installation, which accommodates various virtual machines, of which one is the DDMC. The server is where the virtual machines are configured, provisioned, and managed.
- One of the following:
 - ESXi 5.5
 - ESXi 6.0
 - ESXi 6.5
 - ESXi 6.7
- vSphere client, a Windows-based GUI interface that enables users to connect remotely to any of the server types to perform remote management.

Storage for the VMware installation can be provided using:

- NAS (Virtual Disks over NFS)
- SAN (Virtual Disks over VMFS)

High Availability (HA) requirements

If an HA configuration is required, use the VMware software option of your choice to implement this configuration.

Additional VMware software applications

DDMC is a VMware vApp. In order to improve the reliability of your DDMC installation, you might find the following applications helpful.

VMware vSphere High Availability (HA)

VMware vSphere High Availability (HA) provides cost-effective high availability for any application running in a virtual machine, regardless of its operating system or underlying hardware configuration.

VMware vSphere Fault Tolerance (FT)

VMware vSphere Fault Tolerance (FT) provides zero downtime, zero data loss, and continuous availability for applications, without the cost and complexity of traditional hardware or software clustering solutions.

Backing up and restoring

Any process that creates and restores a *snapshot* of your entire virtual machine can successfully protect your DDMC installation.

It is highly recommended that you perform a snapshot before doing an upgrading procedure.

DDMC does not depend on having any integration with the backup software.

After the snapshot is restored, DDMC automatically performs any necessary application recovery.

Suitable backup software choices would include VMware Data Recovery (VDR), Avamar, and so on.

As with any data protection software, ensure to test your setup after you have installed your chosen backup software.

 **NOTE:** The use of cloning has not been validated.

Getting Started

Topics:

- Prerequisites
- Downloading DDMC
- Installing DDMC in a VMware environment
- Powering on DDMC
- Logging in and out of DDMC
- Continuing DDMC configuration
- Understanding RBAC in DDMC
- Viewing DDMC page elements
- Navigating a DDMC page
- Organizing the dashboard
- Organizing managed Data Domain or PowerProtect systems
- Assigning properties
- Displaying property information
- Managing groups
- Managing replication lag threshold policies
- Working with filters

Prerequisites

Review the chapter [Planning the DDMC environment](#) on page 10 and ensure the required VMware hardware and software components are in place at the site. The guide also includes descriptions of optional VMware software for backup and reliability that ensures the DDMC installation is operating optimally.

Ensure the following are in place:

- VMware vCenter or ESX servers and software
- VMware vSphere client application (VMware vSphere client application are only required if installing on vSphere/vCenter. They are not required for AWS/Azure/GCP/Hyper-V/KVM.)
- Sufficient CPU, memory, disk space, and network resources
- If installing within a Hyper-V or cloud environment, and you cannot use role-based credentials, have information available to create an access profile.

Downloading DDMC

The DDMC file that you use depends upon the environment in which you are operating.

About this task

 **NOTE:** AWS and Azure are supported through the public domain. You have a choice to directly access files or to download files.

Steps

1. Download the DDMC files from the online support site as applicable:
 - ESXi: .ova file
 - Hyper-V: ddmc-<version>-hyperv.zip
 - Azure: ddmc-<version>-azure.zip
 - AWS: ddmc-aws-<version>-osdisk.vmdk

- GCP: ddmc-gcp-<version>.zip
- KVM: ddmc-kvm-<version>.tar.gz
- Vcenter: ddmc-<version>-vcenter.zip

2. Log in to the support site using your existing credentials, or register to obtain your credentials.
3. Select **Support by Product** below the Search box.
4. Use the **Find a Product** search box to find **DDMC**.
5. In the list of categories under the Search box, select **Downloads**.
6. Select the link to download the appropriate version of the software.

Next steps

You can now install the DDMC software on your VMware platform.

Installing DDMC in a VMware environment

There are two procedures for installing the `.ovf` file and configuring settings for DDMC.

- [Installing on a VMware vCenter Server](#) on page 14
- [Installing on a VMware ESX server](#) on page 15

Here is a summary of the factory default settings and the settings that can be configured during the configuration procedure.

Table 3. Installation and configuration settings

Setting	Defaults
Name	Name for DDMC Virtual Machine (default is DDMC)
Hostname	Fully qualified hostname
Gateway IP Address	IP address of gateway server
Serial Number	Auto-generated
IP allocation policy	DHCP or fixed IP address. If fixed, supply the IP address, netmask, and gateway information.
DNS Servers	DNS primary and secondary server names (required). If only a primary is used at the site, type the primary name in the secondary field as well.
Mail Server	Mail server address for the site
Admin Email	Admin email address for the site
ASUP to Support	On (default) or Off
Alerts to Support	On (default) or Off
ASUP to Admin	On or Off (default)
Alerts to Admin	On or Off (default)
AM Email to Admin	On or Off (default)
Network Ports	eth0a – enabled for DHCP; eth0b – disabled
SSH, HTTP, HTTPS	Enabled by default
ASUP and Alerts	autosupport@autosupport.datadomain.com
AM Email	Runs daily at 8 AM
ASUP	Runs daily at 6 AM
sysadmin password	Default is "changeme." After initial login, the password should be changed to something that meets the site's security requirements. Be sure to do this step before you start adding Data Domain or PowerProtect systems.

Installing on a VMware vCenter Server

Prerequisites

1. Download the DDMC software, as described in [Downloading DDMC](#).
2. Open the vSphere client, type the following, and select **Login**:
 - The IP address or hostname of the VMware vCenter Server where DDMC will be installed
 - The administrator ID and password for the VMware server

About this task

 **NOTE:** The following table corresponds to the VMware wizard.

Table 4. Installing DDMC on a VMware vCenter Server

Deployment wizard step	Description
Launch virtual machine deployment wizard	Use the VMware deployment wizard to deploy the DDMC instance.
OVF Template Details	Deploy from the .ovf file or unzip vCenter folder to get .ovf and vmdk files.
Name and Location	Optionally type a name (default is "DDMC"), and select an installation location. This name identifies the virtual machine on the VMware server. It does not become a hostname on the LAN.
Deployment Configuration	Default configuration cannot be changed.
Host/Cluster	Select a host or cluster for DDMC installation.
Datastore	Select the datastore where data is to be stored. For best performance, Data Domain recommends that you use a dedicated datastore.
Disk Format	Select the disk format type. Thin Provisioned disk format dynamically allocates storage capacity. Thick Provisioned disk format allocates all storage now (recommended).
IP Address Allocation	Select the IP address configuration. Either Fixed or DHCP . DDMC does not support Transient . A Fixed IP address configuration also includes network mask, gateway IP address, and primary and secondary DNS server address.
Properties	<p>Provide the following system details:</p> <ul style="list-style-type: none"> • System Identification - Host name: Requires a fully qualified DDMC hostname • Network Information - IP Address: DDMC IP address • Network Information - Network Mask: DDMC network mask • Network Information - Gateway IP Address: DDMC gateway IP address • Network Information - Primary DNS Server: DDMC primary name server IP address • Network Information - Secondary DNS Server: DDMC secondary name server IP address • Email Notification - Mail Server: Requires a hostname for the mail server DDMC will use to send emails • Email Notification - Alerts: Send alert notifications • Email Notification - Autosupport: Send autosupport information • Administrative Contact - Administrator's Email: Requires an email address for a DDMC administrator • Administrative Contact - Alerts: Send alert notifications to the administrator email address • Administrative Contact - Daily Alert Summary: Send the daily alert summary to the administrator email address • Administrative Contact - Autosupport: Send autosupport information to the administrator email address

Table 4. Installing DDMC on a VMware vCenter Server (continued)

Deployment wizard step	Description
Ready to Complete	Review the configuration summary and finish the wizard.

This initial configuration cannot be repeated to change settings. After you have completed an initial configuration, you must use the DDMC CLI for any settings that you want to change.

Installing on a VMware ESX server

Prerequisites

1. Download the DDMC software, as described in [Downloading DDMC](#).
2. Open the vSphere client, type the following, and select **Login**:
 - The IP address or hostname of the VMware vCenter Server where DDMC will be installed
 - The administrator ID and password for the VMware server

About this task

 **NOTE:** The following table corresponds to the VMware wizard.

Table 5. Installing DDMC on a VMware vCenter Server

Installation step	Description
Launch virtual machine deployment wizard	Use the VMware deployment wizard to deploy the DDMC instance.
OVF Template Details	Deploy from the <code>.ovf</code> file or unzip vCenter folder to get <code>.ovf</code> and <code>vmdk</code> files. .
Name and Location	Optionally type a name (default is "DDMC"), and select an installation location. This name identifies the virtual machine on the VMware server. It does not become a hostname on the LAN.
Deployment Configuration	Default configuration cannot be changed.
Datastore	Select the datastore where data is to be stored. For best performance, Dell EMC recommends that you use a dedicated datastore.
Disk Format	Select the disk format type. Thin Provisioned disk format dynamically allocates storage capacity. Thick Provisioned disk format allocates all storage now (recommended).
Ready to Complete	Review the configuration summary and finish the wizard.

This initial configuration cannot be repeated to change settings. After you have completed an initial configuration, you must use the DDMC CLI for any settings that you want to change.

Hyper-V

This version of DDMC enables you to create virtual machines using Microsoft Hyper-V for Windows.

Deployment requirements for Hyper-V

DDMC in Hyper-V uses 4 CPU, 8G RAM, and 250 GB of disk space when deployed.

Set up Hyper-V

Set up Hyper-V by going to Microsoft's Windows Server (2012 R2 or 2016) site and following the instructions that are found on the install page.

Download the Hyper-V package for DDMC

Go to the support site and download the Hyper-V .zip file for your version of DDMC to the Hyper-V server.

Deploying the Hyper-V package for DDMC

About this task

The Hyper-V package consists of the following:

- `ddmc-installer-sc.ps1`: the PowerShell script used for the deployment of DDMC on Microsoft System Center
- `README.txt`: Contains additional information about the steps that are needed to deploy the package.
- `ddmc-N.N.N.N-xxxxxx.vhd`: the boot disk
- `ddmc-installer.ps1`: the PowerShell script needed for DDMC deployment on a Microsoft Windows Server 2012 R2 or Windows Server 2016 with Hyper-V Server.

Steps

1. Unzip the `ddmc-N.N.N.N-xxxxxx-hyperv.zip` package to a folder.
The script must be downloaded onto the Windows server (2012 R2 or 2016).
2. Open the Power Shell prompt as an administrator.
3. Run the following script and specify the name of DDMC virtual machine when prompted: `.\ddmc-installer.ps1`

DDMC on kernel-based virtual machine

DDMC on kernel-based virtual machine (KVM) only supports Intel-based processors. The following Linux distributions are supported.

Table 6. Supported Linux distributions

Linux distribution	Version
RedHat	7.2 and 7.3
SUSE	SLES 12-SP2
Ubuntu	14.04 and 16.04

Deploying DDMC on kernel-based virtual machine

Prerequisites

Steps

1. Download and extract the KVM installable Zip file. File name is `ddmc-kvm-<branch number>-<build number>.tar.gz`.
2. Copy the tar file to the Linux system where KVM is installed, and in partition where VMs are stored. Make a new directory for new DDMC VM.
3. Untar the tar file. It creates a directory.
This directory has the following files:
 - `DDMC_README.txt`: Help file for deploying VM on KVM.
 - `kvm-ddmc-installer.sh`: DDMC deployment script, which automatically setups CPU, RAM, DISK, NVRAM configuration
 - `ddmc-<branch number>-<build number>.qcow2`: Root disk for VM

```
root@ddve-ucs55d:/mnt/ucs55d-das1/ddmc_set/ddmc1# tar -xzvf ddmc-kvm-0.6120.12.0-566688.tar.gz
```

```
ddmc-kvm-0.6120.12.0-566688/
ddmc-kvm-0.6120.12.0-566688/DDMC_README.txt
ddmc-kvm-0.6120.12.0-566688/kvm-ddmc-installer.sh
ddmc-kvm-0.6120.12.0-566688/ddmc-0.6120.12.0-566688.qcow2
```

4. Run `kvm-ddmc-installer.sh` script to deploy DDMC VM. Once the VM is deployed, it will power on.

```
root@ddve-ucs55d:/mnt/ucs55d-das1/ddmc_set/ddmc1/ddmc-kvm-0.6120.12.0-566688# ./kvm-ddmc-
installer.sh
Distribution:ubuntu Version:16.04
The host version check done.
Basic validation done.
Convert the root disk to raw...
Disk convert done.
root disk:/mnt/ucs55d-das1/ddmc_set/ddmc1/ddmc-kvm-0.6120.12.0-566688 config type:4TB
bridge:br0
Start creating DB disk, it may take a few minutes...
DB disk file has been created successfully.
Domain ddmc-0.6120.12.0-566688 defined from config.xml

Domain ddmc-0.6120.12.0-566688 marked as autostarted

Domain ddmc-0.6120.12.0-566688 started

DDMC instance has been created successfully!
```

5. Log in to the GUI of KVM host. Run `virt-manager` command, and the KVM GUI to manage VMs should appear.
6. Connect to console, and check IP the address. DDMC can now be remotely configured.

Adding Dell EMC PowerProtect DD Virtual Edition to DDMC

Steps

1. Deploy PowerProtect DDVE on KVM. (For more information, see the appropriate DDVE installation and administration guide.)
2. Get the IP addresses of the DDVE to be added to DDMC for management.
3. Log in to DDMC.
4. Run the following command on DDMC to add managed DDVE system DDVE to DDMC, # `managed-system add <IP address of DDVE> inbound-proxy <IP address of DDMC> outbound-proxy <IP address of DDVE>`.

```
managed-system add 10.98.99.237 inbound-proxy 10.98.99.225 outbound-proxy 10.98.99.237
The SHA1 fingerprint for the remote host's CA certificate
is46:3D:3C:B3:38:CE:31:E1:CE:1B:E6:4B:41:42:D3:78:00:D9:01:60
Do you want to trust this certificate? Are you sure? (yes|no) [no]: yes

** Once added, all "admin" role users on this DDMC
will operate on "10.98.99.237" system with "admin" role.
And all "limited-admin" role users on this DDMC
will operate on "10.98.99.237" system with "user" role if the system version is 5.7
and below, or "limited-admin" role if the system version is 6.0 and above.
```

```
To allow "10.98.99.237" to be managed by this DDMC,
Enter "10.98.99.237" sysadmin password: ok, proceeding.
10.98.99.237 is added.
It may take a while to collect all information for "10.98.99.237".
sysadmin@ddmcset-ddmc-1# managed-system show
Host Name                Serial Number    State    Status    DD OS Version
Sync Time                Type
-----
ddmcset-ddve-1.datadomain.com  AUDVTPCKZ1SY5W  managed  online    0.6120.12.0-564400
Jun  6 2017 12:22  standalone
```

5. In a supported browser, type `http://<IP address of DDMC>` to connect to DDMC GUI.

Results

The DDVE system is added under **Systems > Inventory**.

Manageability in public cloud

This version of DDMC allows for cloud manageability, the creation of virtual machines, and manage capacity through Azure, Amazon Web Services (AWS), and Google Cloud Provider (GCP).

Using Amazon Web Services (AWS) Marketplace Amazon Machine Image (AMI)

The Amazon Machine Image (AMI) can be created in one of two ways: one is through the Amazon Web Services portal and the other is through the CLI. To deploy DDMC from the AWS Marketplace, perform the following steps.

Prerequisites

If you do not already have an Amazon Web Services (AWS) account, contact the AWS administrator.

Account information includes the following:

- Account user ID
- Password
-  **NOTE:** Initial DDMC password for deployment in AWS is the instance ID.
- Access key ID
- Secret access key

Steps

1. Log in to the AWS portal.
2. Select **EC2 Service**.
3. Select the region.
4. Click **Launch Instance**.
5. Select **AWS Marketplace** in the left navigation pane.
6. Search for **Data Domain** and select DDMC.
7. To complete the AMI deployment process, follow the steps in the AWS wizard.

Using the CLI to create Amazon Web Services (AWS) Amazon Machine Image (AMI)

The Amazon Machine Image (AMI) can be created in one of two ways: one is through the Amazon Web Services portal and the other is through the CLI. To create an Amazon Machine Image (AMI) using the CLI, follow these steps.

Prerequisites

If you do not already have an Amazon Web Services (AWS) account, contact the AWS administrator.

Account information includes the following:

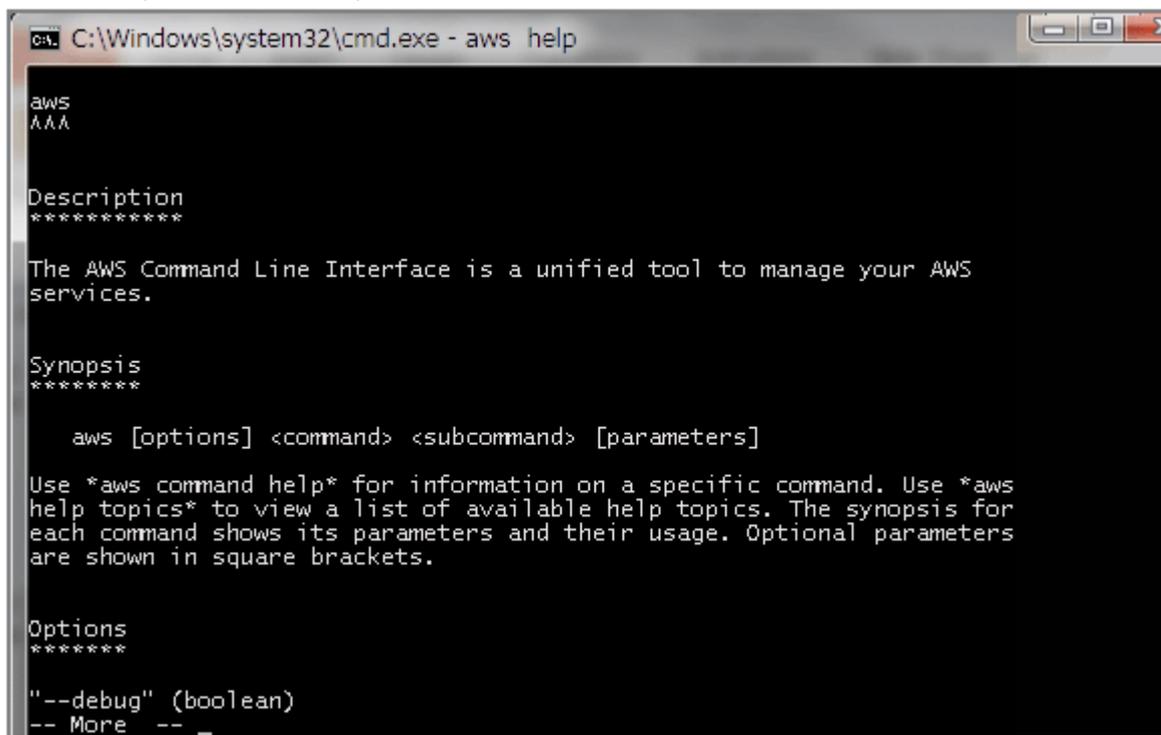
- Account user ID
- Password
-  **NOTE:** Initial DDMC password for deployment in AWS is the instance ID.
- Access key ID
- Secret access key

Steps

1. Download and install the [AWS CLI tool](http://docs.aws.amazon.com/cli/latest/userguide/installing.html), which is available for Windows and Linux (<http://docs.aws.amazon.com/cli/latest/userguide/installing.html>).

2. Verify that the tool is installed by opening a terminal, shell, or command prompt and entering the following command: `aws help`

The AWS help text should be displayed:



```
C:\Windows\system32\cmd.exe - aws help

aws
AAA

Description
*****

The AWS Command Line Interface is a unified tool to manage your AWS
services.

Synopsis
*****

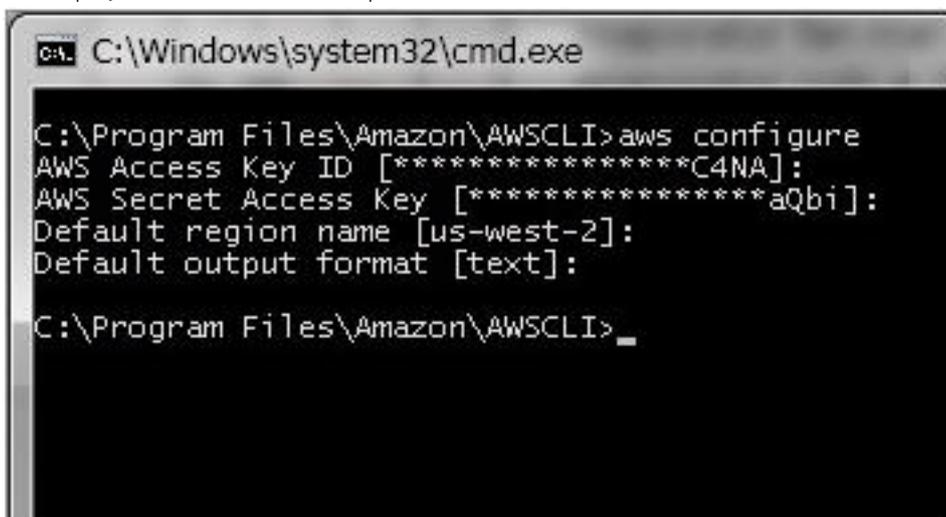
    aws [options] <command> <subcommand> [parameters]

Use *aws command help* for information on a specific command. Use *aws
help topics* to view a list of available help topics. The synopsis for
each command shows its parameters and their usage. Optional parameters
are shown in square brackets.

Options
*****

"--debug" (boolean)
-- More --
```

3. Using the command line tool, run `aws configure` and paste in the access key ID and secret key when prompted. Subsequent logins have default values based on the last successful login. The region setting is where the DDMC is uploaded and deployed, and the default output format should be JSON.



```
C:\Windows\system32\cmd.exe

C:\Program Files\Amazon\AWSCLI>aws configure
AWS Access Key ID [*****C4NA]:
AWS Secret Access Key [*****aQbi]:
Default region name [us-west-2]:
Default output format [text]:

C:\Program Files\Amazon\AWSCLI>
```

4. Download the DDMC or VMDK (VM disk image file format) for AWS of choice from Online Support to the same system where AWS CLI is installed.
Linux example: `cp ddmc-aws-0.19.100.0-551712-osdisk.vmdk <your AWS folder>`
5. Upload this VMDK to the appropriate S3 bucket: `aws s3 cp <downloaded ddmc vmdk name> s3://<your images bucket>/<downloaded ddmc vmdk name>`
`aws s3 cp ddmc-aws-0.19.100.0-551712-osdisk.vmdk s3://ddmc-image-bucket/ddmc-aws-0.19.100.0-551712-osdisk.vmdk`
6. Create or edit `containers.json` to use the file name of the VMDK for the "S3Key." This JSON file should be in the same folder as the AWS CLI and have the following contents:

```
{
  "Description": "DDMC Import",
  "Format": "vmdk",
```

```
"UserBucket": {
  "S3Bucket": "xxxx-xxxx-xxxxxx",
  "S3Key": "ddmc-aws-0.19.100.0-551712-osdisk.vmdk"
}
```

Be sure to replace the S3Key field with the VMDK file name and that you are using the correct S3Bucket name.

7. Create the Amazon Machine Image (AMI) by using the uploaded VMDK and the CLI:

```
aws ec2 import-snapshot --description "ddmc import" --disk-containers file://
ddmc_import.json
```

To check progress of the new task that was just created, note the "ImportTaskId" value from the JSON returned by the above command, and use it in the following command:

```
aws ec2 describe-import-snapshot-tasks --import-task-ids import-snap-ffje91fn
```

8. Once it is done, look for the Status Message "completed" and note the snap-ID.

Deploying DDMC with Amazon Web Services (AWS)

To deploy DDMC in Amazon Web Services (AWS), follow these steps.

Prerequisites

If you do not already have an Amazon Web Services (AWS) account, contact the AWS administrator.

Account information includes the following:

- Account user ID
- Password
-  **NOTE:** Initial DDMC password for deployment in AWS is the instance ID.
- Access key ID
- Secret access key

Steps

1. Open a web browser, and go to <https://ddltr.signin.aws.amazon.com/console>. Log in with user ID and password. Select the appropriate region.
-  **NOTE:** If the VMDK was manually converted, the selected region must match the region from the conversion process.
2. Prepare to launch the instance by selecting the **Services** drop-down on the left side, then choose **EC2**.
3. From the navigation pane on the left side, select **Snapshots** under **Elastic Block Store**.
4. If the CLI was used to create the AMI, locate the [snapshot ID](#).
5. Click **Actions > Create Image**.
6. In the new dialog box, name and describe the new image. Be sure to select the **Hardware-Assisted Virtualization** option.
7. Once the image is created, use the AMI ID to locate the image and launch the VM.
8. Click the **Add New Volume** button, set the **Volume Type** to **EBS** and the **Size** to **200GiB**, tick the two boxes for **Delete on Termination**, then click **Next: Add Tags**.
9. Add a value for **Name** (following established naming conventions), then click **Next: Configure Security Group**.
10. Select a security group that has SSH, HTTPS, and RDP ports open, then click **Review and Launch**.
11. Click the **Launch** button. You may safely ignore the warning about free usage tier eligibility.
12. Type the security key pair. This information is needed when accessing the DDMC over SSH. Click **Launch Instances** and then **View Instances** when it starts launching.
13. Locate the instance name from step 12, click it and note its IP address below the list.

Results

When the instance has finished booting, it may be accessed in the VPC and subnet selected earlier.

- Local network policy may block access to these subnets and ports. In this case, an alternate network must be used.

- Initial DDMC password for deployment in AWS is the instance ID.
- For command-line access, an SSH client (such as PuTTY) may be used with the key pair from step 12.
- For GUI access, a web browser can be used if it is in the same subnet.
- Cloud-based DDVEs can be now added to the DDMC.

Deploying DDVE systems

Introduction

The DDMC provides new REST APIs to automate managing the life-cycle of DDVE systems running in Amazon Web Services (AWS).

The DDVE life-cycle management APIs enable you to integrate cloud-based DDVEs into your cloud operations systems. The APIs enable you to:

- Securely manage AWS credentials
- Deploy DDVE instances
- Provision EBS storage for the file system
- Ensure DDVEs are consistently deployed
- Deprovision and destroy DDVEs when they are no longer needed

Installation and prerequisites

The DDVE deployment APIs are delivered as part of the DDMC. DDMC runs as a virtual machine, separate from the DDVEs and DD Systems it is managing. DDMC can run on-site hypervisors (ESX, vCloud, Hyper-V, or KVM) or as a VM in AWS or Azure. See the DDMC installation guide for details.

In order for DDMC to manage cloud DDVEs, it requires an unblocked network access to invoke AWS APIs and the DDVE APIs (port 3009 on the DDVE, accessed through HTTPS).

DDVEs need a license to ingest and restore data. Rather than install individual license files, the DDMC configures DDVEs that use a license server. You need to install a license server and configure DDMC to learn about the server. You also need to install a served license file on the license server with sufficient capacity for your intended deployment.

Managing Amazon Web Services (AWS) credentials

To deploy DDVEs and provision storage, DDMC needs to be able to invoke AWS APIs. AWS requires an API caller to present credentials to authenticate the caller before running the API .

To prevent security issues, the DDMC has two ways to access AWS credentials. The first, and most secure, method is to run DDMC as an AWS virtual machine. If you configure the DDMC with the AmazonEC2FullAccess, AmazonS3FullAccess, and IAMFullAccess permissions, this enables DDMC to invoke AWS APIs using a temporary set of credentials.

If you cannot use role-based credentials, you can create an Access Profile. The Access Profile securely stores the AWS public key and secret key in the DDMC database. When a user invokes the DDVE deployment API, DDMC uses the named set of credentials to deploy the DDVE and provision storage. You can create as many Access Profiles as you need using the `/rest/v1.0/system/vi/access-info` URI. You operate on access profiles using the standard POST, PUT, GET, and DELETE operations.

Preparing the DDVE Amazon machine image

Before you can deploy a DDVE, you have to create an Amazon Machine Image (AMI). The DDVE code is delivered as a VMware virtual drive file (VMDK). Amazon has tools to convert this file into an AMI. In brief, you transfer the DDVE boot disk image to a S3 bucket and use the Amazon tools to convert this file to an AMI. When done, the AMI is assigned an AMI ID. You need this ID as part of the deployment process.

Managing virtual resources

You can deploy many DDVEs using the same set of hardware resources. DDMC enables you to create a collection of resources to be used in every deployment to maintain consistency. This object is called a resource profile. In AWS, the resource profile specifies:

1. The AWS region, such as "us_east_1"
2. The name of the AMI to use for deployments
3. The AWS subnet ID
4. The AWS security group

See the AWS documentation for more information about the region, subnet ID, security group, and AMI ID. The AMI ID is the ID you get when you create the DDVE AMI. Resource profiles are managed through the /rest/v1.0/system/vi/resource URI.

Creating a DDVE configuration template

The deployment process applies a configuration template to a newly deployed DDVE. The configuration template defines a set of DD OS settings you would like to be consistently applied to your Data Domain or PowerProtect systems. The template is stored in the DDMC database. The configuration template has sections for network settings, alert notification, time settings, DD Boost, and more.

To create a configuration template, you must first deploy a Data Domain or PowerProtect system, configure, and test it, then extract a template from that system. You create configuration templates using the POST /rest/v1.0/system/config/templates API, passing in a name for the template and the name of a Data Domain or PowerProtect system from which to extract the template. Refer to Appendix B.

Deploying a DDVE

After all the preparation steps, you are ready to deploy a DDVE. When deploying a DDVE, DDMC runs a workflow with several steps. The workflow steps are as follows:

1. Creating and booting an AWS virtual machine using the DDVE AMI .
2. Provisioning EBS volumes to hold the file system data and attaching those volumes to the DDVE.
3. Configuring the DDVE to use a license server.
4. Setting the DDVE hostname, IP address, and sysadmin password.
5. Creating a Data Domain or PowerProtect file system on the EBS volumes.
6. Applying an optional configuration template.
7. Adding the DDVE to the DDMC inventory.

You initiate the process by running a POST to /rest/v2.0/dd-systems. This is an updated API for this release. The request body includes a new structure which tells DDMC to deploy a DDVE. The request structure looks like this:

```
POST /rest/v2.0/dd-systems
{
  "hostname": "my-ddve-hostname",
  "password": "abc123",
  "deploy_info": {
    "environment": "aws",
    "common_deploy_info": {
      "vm_name": "my-ddve-name",
      "access_profile_name": "aws_access_profile",
      "resource_profile_name": "resource_profile",
      "config_template": "configuration_template_name"
    },
    "aws_specifc_deploy_info": {
      "init_config": 2,
      "max_config": "8TB"
    }
  }
}
```

See the online REST documentation for an explanation of the fields. The AWS and legal values and descriptions are as follows.

Table 7. AWS, legal values, and descriptions

Field	Legal values	Description
init_config	Unsigned integer between 1 and max config size	Capacity of the file system when initially deployed in TiB

Table 7. AWS, legal values, and descriptions (continued)

Field	Legal values	Description
max_config	"8 TB," "16 TB-A" and "16 TB-B"	The maximum allowable capacity of the file system; all DDVEs will be provisioned and licensed with a 500 GiB evaluation license

This takes several minutes to complete. Ensure that the REST client has a sufficiently long timeout.

While the deployment is running, you can monitor its progress by running a GET on /rest/v1.0/tasks URI to see a list of all (or active) tasks. From the task list, you can retrieve a task ID and use that id to GET /rest/v1.0/tasks/{ID} to get the detailed status of the running task.

Managing a DDVE

Once the DDVE is deployed, you can monitor and manage it using all the standard DDMC interfaces. You can monitor status, health, capacity and much more through the DDMC GUI. You can launch System Manager to make changes to the DDVE. Also, there are many DDMC REST APIs you can use to do things like provision MTrees, create NFS exports, build your own performance monitoring applications, and perform delete/deploy functions. Refer to Appendix B.

Destroying a DDVE

When you are done with the DDVE, use the DELETE /rest/v1.0/dd-systems/{SYSTEM-ID} API to remove the DDVE from the DDMC inventory. In addition to removing the system from the inventory, DDMC destroys the DDVE and deprovision the EBS storage that is used for the file system. Again, this is a long running task which you can monitor using the /rest/v2.0/tasks URIs. Refer to Appendix B.

DDMC in Azure Marketplace

About this task

Perform the following steps to deploy DDMC from the Azure Marketplace.

Steps

1. Log into the Azure portal.
2. Select **Virtual Machines** from the left pane.
3. Click **Add**.
4. Select **Dell EMC PowerProtect DD Management Center (DDMC)** from the Azure Marketplace.
5. Click **Create**.
6. Complete the settings information under **Basics**. Click **OK**.
7. Choose Standard_D2 size. If not visible on the page, click View All. Click Select
8. Under **Storage** and **Network** settings, provide details on the storage account, virtual network, subnet, and network security group. Keep High Availability, Storage (Use managed disks), and Public IP Address as **None/No** as shown in the example. Keep diagnostics off and only turn them on when required. To keep diagnostics logs, specify the storage account. Click **OK**.
9. Click **Purchase**.
10. Wait for VM to successfully deploy. If there is any error, the problematic parameter is mentioned in the error.

DDMC in Google Cloud Platform

Prerequisites

1. Get Gmail ID enabled to access Google Cloud Platform (GCP).
2. Collect details of Jumpbox that can be used to access VMs in GCP.
 - VPC

- Subnet
- Region

Steps

1. Sign in to Google Cloud Platform, and select or create a GCP project.
2. Create a bucket by going to **Storage > Browser > Create Bucket**.
 - a. Enter a unique **Name** for your bucket.
 - Bucket names must contain only lowercase letters, numbers, dashes (-), underscores (_), and dots (.). Names containing dots require verification.
 - Bucket names must start and end with a number or letter.
 - Bucket names must contain 3–63 characters. Names containing dots can contain up to 222 characters, but each dot-separated component can be no longer than 63 characters.
 - Bucket names cannot be represented as an IP address in dotted-decimal notation (for example, 192.168.5.4).
 - Bucket names cannot begin with the "goog" prefix.
 - Bucket names cannot contain "google" or close misspellings, such as "g00gle".

Also, for DNS compliance and future compatibility, you should not use underscores (_) or have a period next to another period or dash. For example, ".." or "-." or ".-" are not valid in DNS names.
 - b. Choose **Regional** for **Storage class**.
 - c. Select the **Location** where the DDMC instances are running.
 - d. Click **Create**.
3. Collect Access keys and secret keys from GCP console by going to **Storage > Settings > Interoperability**. Note the **Storage access keys**.
4. Set up Google Cloud SDK in your local system.

Cloud SDK requires Python 2.7.x.

 - a. Download SDK from GCP SDK.
 - b. Extract files.
 - c. Append these files with the following certificates:
 - platform/bq/third_party/httplib2/cacerts.txt
 - platform/gsutil/third_party/boto/boto/cacerts/cacerts.txt
 - platform/gsutil/third_party/boto/tests/integration/s3/other_cacerts.txt
 - platform/gsutil/third_party/httplib2/python3/httplib2/cacerts.txt
 - platform/gsutil/third_party/httplib2/python2/httplib2/cacerts.txt
 - platform/gsutil/gslib/data/cacerts.txt
 - lib/third_party/httplib2/cacerts.txt
 - lib/third_party/httplib2/python3/httplib2/cacerts.txt
 - lib/third_party/httplib2/python2/httplib2/cacerts.txt

```

-----BEGIN CERTIFICATE-----
MIIEzDCCA7SgAwIBAgIQfzDeHUGOUzX68dftXnBR9zANBgkqhkiG9w0BAQsFADA9
MQswCQYDVQGEwJVUzEYMBYGA1UEChMPRU1DIENvcnBvcnF0aW9uMRQwEgYDVQQL
EwtFTUMgUm9vdCBDQTAeFw0xNTEwMTUxNzAwMzJaFw0yNjAzMDYwMjM5MzNaMHgx
CzAJBGNVBAYTA1VTMRgwfG9FTUMgQ29ycG9yYXRpb24xJTAjBgNVBAsT
HEdsb2JhbCBTZWN1cm10eSBPcm9udHBM16YXRpb24xKDAmBgNVBAMTH0VNQyBTU0wg
RGVjcnlwdG1vbiBBdXR0b3JpdHkgdJiWggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQQDJvnnKsIWctCm1m1P53fHpAnCmPfTgtGICGj1dgM2osz5Y0TZRqf57
OefJaE9uZCFr2DMPR90s1mI3ybdpgA/EA6bGDdepW3jLCn7y8uVFZ94xLr3Hv5Xe
fzIUnUXakmIbGmKfBfhVLHQfY22RDks5RNCj/Y+Q0xGbJvjKzes+FnGkMy5WdJ5P
kz8Awlbz26HVX1lh4+7KEcfjV1lyNtMh1Sk7KJmVChlRvof4u40AI7AwHamm7D4R
3BhiMzHpj1NO5tb4exd1Y6Y38pDFaIJGCDe4irdaiYg3dUSYv7oPazFCv7ng4aNR
hwPyTjAhWSXWC4kkZqgECEmeRdgX5CXxAgMBAAGjggGLMIIBhZCCAR8GA1UdHwSC
ARYwgGESMDWgM6Axi9odHRwOi8vcGtpLmNvcnAuZW1jLmNvbS9jcmwvRU1DJTiw
Um9vdCUyMENBLmNybDA6oDigNoY0aHR0cDovL2VudGVycHJpc2VjYS5jb3JwLmVt
Yy5jb20vRU1DJTiwUm9vdCUyMENBLmNybDcBnKCBmaCBloaBk2xkYXA6Ly8vQ049
RU1DIFJvb3QgQ0EsQ049RU1DIFJvb3QgQ0EsQ049Q0RQLENOPVB1YmxpYyBLZXkg
U2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdG1vbiEQz1lbWNyb290
LERDPVwtYyxEQz1jb20/Y2VydG1maWNhdGVsZXZvY2F0aW9uTG1zdDAOBgNVHQ8B
Af8EBAMCAyYwHwYDVR0jBBgwFoAUjyKad6YrWTr8z+fAlE5VRpSg/zQwEgYDVR0T
AQH/BAgwBgEB/wIBAjAdBgNVHQ4EFgQUpcg3w8f5h2Sazw2ogrJNxM5u9UMwDQYJ
KoZiHvcNAQELBQADggEBAKDr+Kz19+Dw7bn+qm4+TZuR0g30pEiGov7i30D6hNL7

```

```
XSPzGRmQYXEmucEEsomy6iBMAPmLqdWfFBDh2vSmnOGk0IL+q3WzLq6IGPpXI4Wf
GGAnjujnPsk6YF1OyrqYlVN0BUPQ3Jz8l3OI1Ga0/2RM5jogkCqsZSoaHdNrouk
mA5Rz0cgETyU5TXC/+a6CEqDbFviqaiiHHZvjCVlgKmdQXirEPm6b2vp2B/DBiVW
6eTyDrIGle10RuPZTKSmlEWSgTshyMCNdOFLm7TsSkgbLgWwWfYDOeCHhvZdEuqP
dApqEUwXn00ppEt1jo5zvCLsYmkri4bxanMGHBcgG9o=
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
MIIDajCCAlKgAwIBAgIQDnpJf/sai2ikg8QrEDRcejANBgkqhkiG9w0BAQUFADA9
MQswCQYDVQQGEwJVUzEYMBYGA1UEChMPRU1DIENvcnBvcnF0aW9uMRQwEgYDVQQD
EwtFTUMgUm9vdCBDQTAeFw0xMTAzMDgwMjM1MTThaFw0yNjAzMDgwMjM1MTThaMD0x
CzAJBgNVBAYTAlVTMRgwFgYDVQQKEw9FTUMgQ29ycG9yYXRpb24xFDASBgNVBAMT
C0VNQyBSb290IENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwEV0
QaykbhIOVKj1BunB8pXsISlXgivl0QSGSxG2Dnbwoli0WSgPpLqPD8bsQuwjReg0
ERGXTXpxDEpb4Kya+YcIr4KGMd+EIIdLjogXnrKv1/EWa54UNNjNLU6tkwEnVQ79p
Sbx2weCxEi+VG755+Bbb5AJKDCgk4ss5hXjI8tOzAgHe+tRenQamMSOgCO+4bZJ1
RBalcYHmGxVz2TbK0qrKkC7Um4ALQfRQejB+TuvYMoTZHD8Wm/e3Hdq7wwTOMQUL
/hG4+J+k4f18WUf4M6CzmeYVnEpZ34wk4H/1bRmFI9jvEQlmu/uKmFZ8DPOvK8j
YJCPft/fWOLkCZOSPwIDAQABO2YwZDAOBgNVHQ8BAf8EBAMCAYYwEgYDVR0TAQH/
BAGwBgEB/wIBAzAdBgNVHQ4EFgQUjyKad6YrWTr8z+fAlE5VRpSg/zQwHwYDVR0j
BBgwFoAUjyKad6YrWTr8z+fAlE5VRpSg/zQwDQYJKoZIhvcNAQEFBQADggEBALaL
B5rAo9GLri9vvYMIkMwtI4SFYeftNrY47YA4o49sbCVlgdmzUXWk48aevouzRl6/
rEPfbTxaZUbmjOv+XO+bGFA3T57RS6rAFegBai/UirrcKJhGgusAVU51FtO31Mgm
W3cPXqV+PXwwHKbgLRCeTJFK3Rw68TxBqazMjNp4WufdnPC379Fg/zeKrcLwgsa4
AVFHmeIadvijSQBpY0bFzssZGF/PmAh+NiYJpWRdDXfeeQStdZWxPESbWoXPu/Qg
0dIifLaHr2Nugkg8eTcP+F2rl2YIjnQcEFqOUNhyI8kPzssWinYel47tC9kDL7qR
s34MLubs2L1iMIk7fJ4=
-----END CERTIFICATE-----
```

- d. Run `install.sh`.
 - e. Open a new Bash session and run `gcloud init --console-only`.
 - f. Verify the configuration.
5. Using the `gsutil` tool, upload DDMC and DDVE base files to the GCP bucket.
 6. Create boot images for both DDMC and DD VE.
 7. Upload boot gzip files to the GCP bucket.
 8. Deploy DDMC and DDVE VMs in GCP using the boot disk images either from Windows or Linux client where Google SDK was set up.
 9. Verify that the VMs are created and deployed.
 10. Label GCP VM instances by double-clicking on a VM instance.

Powering on DDMC

About this task

If installation is successful, you can power on the DDMC virtual machine and login to the system.

Steps

1. Open the client, and navigate to the location where you configured DDMC.
2. Right-click on the instance, and select **Power On**.
3. Optionally, right-click and select **Console** to view the boot and initialization process. After a successful boot sequence completes, a CLI prompt is displayed. You can log in as **sysadmin** with the initial password **changeme**.

 **NOTE:** While the CLI can be used to log in to DDMC and perform some operations (see "[Differences between DDMC CLI and DD OS CLI](#)" on page 128"), the preferred interface for working with DDMC is the GUI.

Logging in and out of DDMC

DDMC is accessed by using a supported browser on a workstation that has network access to the DDMC instance. DDMC supports multiple simultaneous users.

The following browsers are supported for use with DDMC:

- On Microsoft Windows – Microsoft Internet Explorer 11 and Edge (only on Microsoft Windows 10); Mozilla Firefox 30 and higher; Google Chrome
- On Apple OS X – Mozilla Firefox 30 and higher; Google Chrome

Other browser versions may also work; these particular versions have been validated. See the release notes for the most up-to-date information.

Logging into DDMC

Initial login requires using the "sysadmin" user ID and the "changeme" password (the default password). You are then prompted to change the sysadmin password. After that, other users with different roles (that have been added to DDMC) may login.

About this task

To log in to DDMC:

Steps

1. Open a browser, and enter the hostname or IP address of DDMC.
A **Secure Login** link is provided for establishing a secure connection over the network using HTTPS instead of HTTP. This option uses a self-signed certificate by default, which the user must accept, despite browser warnings.
2. In the login window, enter a user name and password, and press Enter, or select **Log In**.

Results

After you log into DDMC, the Dashboard is displayed, showing the default set of monitoring widgets.

Related concepts

[Managing local user access to DDMC](#) on page 103

[Global controls and icons](#) on page 123

Logging in with Public Key Infrastructure (PKI) and Common Access Card (CAC) certificates

Users can login to DDMC with their existing PKI/CAC and present the Data Domain or PowerProtect system with a certificate for authentication or authorization.

Prerequisites

Logging in with a certificate is only available through a secure login page (HTTPS), and it also requires an import of CA Root and intermediate files through the CLI.

Steps

1. To import CA Root, enter the following command in the Windows or Linux CLI:
`ssh sysadmin@DDMC adminaccess certificate import ca application login-auth < rootCA.crt`
2. To import the intermediate CA files, enter the following command in the CLI:
`ssh sysadmin@DDMC adminaccess certificate import ca application login-auth < intermediateCA.crt`

3. Select the "Log in with certificate" link.

The **Select a Certificate** dialog displays, enabling users to select the appropriate certificate to use to login to DDMC.

NOTE: Only users that exist in DDMC are displayed.

- Certificate supports local, NIS, and AD users.
- Users are authenticated by the Data Domain or PowerProtect system using the public certificate present on the CAC/PKI.
- Using a CAC/PKI card might require the user to enter a PIN as part of the certificate authentication process.

Logging out of DDMC

To log out of DDMC, click the User icon on the DDMC banner and select **Logout** in the dropdown or just close your browser window.

Continuing DDMC configuration

You have completed basic DDMC configuration and are ready to use DDMC.

The basic configuration enables DDMC to be started, but many more settings may need to be configured to fully integrate DDMC into your site.

You may need to configure network settings and routing tables, set the time zone configuration, and provide access for users. All of this information is described in the [Performing additional configuration](#) chapter.

Understanding RBAC in DDMC

DDMC uses role-based access control (RBAC) to control how data is manipulated and displayed both within DDMC and on Data Domain systems that are managed by DDMC.

DDMC users can:

- Have one of three roles within DDMC: *admin* (system administrator), *limited-admin*, or *user* (basic user)
- Have one of four roles on the systems that are managed by DDMC: *admin* (system administrator), *limited-admin*, *user* (basic user), or *backup operator*
- Modify DDMC states only if they have the *admin* or *limited-admin* role
- View data from a system (through DDMC) as permitted by the role they have on that Data Domain system
- Modify a system only if they have the *admin* or *limited-admin* role on that Data Domain or PowerProtect system

Viewing DDMC page elements

DDMC is composed of various page elements.

The three main areas of the DDMC main page are the banner, navigation panel, and the work area.

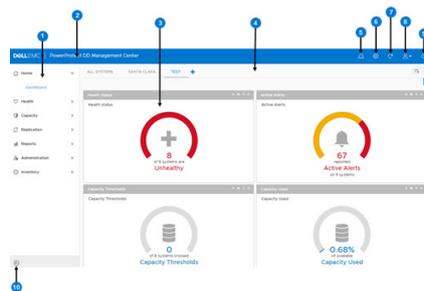


Figure 1. DDMC page elements

1. Navigation panel with module listing
2. Banner with status and control area
3. Dashboard widget
4. Work area
5. Alerts
6. Settings
7. Refresh
8. User profile
9. Online Help control
10. Collapse or expand menu

The navigation panel is organized by module – Dashboard, Health, Capacity, Replication, Reports, Administration, and Inventory. Within each module, you can select the name of a subject page to be displayed in the work area.

Unless the dashboard is maximized, the banner is always visible. It provides controls to filter the scope of the work area's active page (the filter control is displayed only on monitoring pages), open the online help, and log out.

The banner shows alerts notifications (which you can select, to see an informational dialogue window with a link to the Alerts page) and provides the active user, role, and access to classic view of DDMC.

Standard global controls (add, edit, delete) enable interaction with the application and manage how information is displayed on pages with tables (sorting column content by ascending/descending controls, hiding/displaying columns).

Related tasks

[Working with filters](#) on page 41

Navigating a DDMC page

Navigation elements on a DDMC page change the focus and scope of the content that is displayed in the work area.

1. Module topics are found on the left, in the navigation panel.
2. Tabs (if applicable) are found at the upper right, in the banner.
3. Toggle buttons (if applicable) let you change from a standard system list, to a group of systems, to a Tenant view, and so on. If you choose groups, only groups that you have created will be displayed. In this picture, you can choose from a **Systems** or **Groups** view.

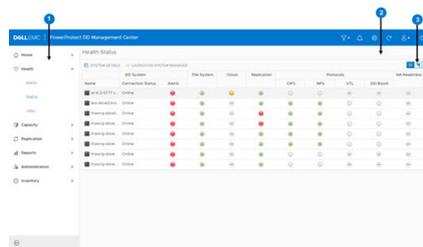


Figure 2. DDMC page navigation

Organizing the dashboard

The dashboard holds *widgets* that you create for a set of monitoring functions. The dashboard lets you quickly check important conditions, such as unreachable systems, active alerts, diminishing capacity, and so on.

You can set up separate *tabs* on the dashboard and include specific widgets for each of those tabs. Suggested uses for tabs are to organize sets of systems based on group membership, location, operating system version, datatype, and so on. Another suggestion is to organize by widget type, for instance, a tab containing Current Health Status widgets for all systems.

By default, each user is assigned a dashboard with one tab, which is populated by one each of the supplied widgets and are configured to cover all the systems that a user is monitoring. You can modify, add to, or even delete this default dashboard tab.

A tab with all of its widgets can be copied to a new tab and then edited.

Adding and configuring tabs

Tabs can be quickly created by clicking the blue plus sign (+) in the banner and completing the required **Name** and **Filter** fields in the **Add Dashboard** window. To customize your DDMC setup, you can add tabs, choosing a unique name, number of columns, and placement.

Steps

1. Select **Home > Dashboard**.
2. On the dashboard, select the **Add tab** control in the banner, in the upper right.
3. In the **Add and Configure Dashboard Tabs** dialog, select **ADD** (green plus sign).

4. In the selected text field, enter the name for the tab.
5. Choose the number of columns for the tab (more columns produce smaller widgets) and any applicable filter.
6. Click **ADD**.
7. Order the placement of the tab across the dashboard using the **MOVE UP** or **MOVE DOWN** controls.
8. Click **SAVE**.

Results

The new tab is displayed on the dashboard.

Adding widgets

You can also add widgets to customize your DD Management center setup.

Steps

1. Select **Home > Dashboard**.
2. On the dashboard, navigate to a tab (All Systems, etc.), or create a new tab (see the preceding section).
3. Select the **Add widget** control in the banner, at the top right.
4. In the **Add Dashboard Widget** dialog, enter a Name that will reflect the widget's use. For example, using a Lag Thresholds template, you could name the widget "New Jersey Lag Thresholds" if you have set filters to show only those systems that replicate to New Jersey. The name must be unique for this tab.
5. Select a Template for the desired output. When you select a template, an image appears under Example, showing an example of a widget of that type.
6. If applicable, in the Settings area, select any of the available options (such as filtering to narrow the scope of the widget monitoring). Widgets can be filtered using standard filter primitives such as systems, groups, and properties. Also, depending on the template, you may have other settings that you can configure.
7. Click **ADD**.

Results

The new widget is displayed on the dashboard.

Widget templates

You can add, edit, or delete widgets from the dashboard, by selecting the Add widget control in the banner at the top right, by using the Edit widget control in the banner of each widget, or by using the Remove widget control in the banner of each widget, respectively.

Health Status widget

The **Health Status** widget shows a summary of important health factors for monitored systems, such as the status of the file system, replication status, alerts, and protocol status.

If all the systems are healthy, a green version of the widget is shown, filling the arc pattern. However, if some of the systems are unhealthy - either in File System, Replication or other areas, a ratio is shown in the Red Graph, and the number below will display the count. Navigation from this widget takes the user to the Health Status page.

Select the Show detail control (>>) to display the **Health > Status** page.

Active Alerts widget

The **Active Alerts** widget shows the distribution of active alerts across all managed systems by type – Emergency & Alert, Critical & Error, and Warning.

If there are no alerts on any of the systems in the inventory, the widget will show an empty arc, and the text color will change to neutral blue. Warning level alerts are shown in yellow, and critical and above are shown in red. If there is at least one alert, the arc will be full; it functions similar to a pie chart. Navigation from this widget takes the user to the Health Alerts page.

Select the Show detail control (>>) to display the **Health > Alerts** page, where a complete list of Health Alerts is displayed.

Capacity Thresholds widget

The **Capacity Thresholds** widget shows the distribution of capacity usage across all managed systems.

This widget shows the count of systems which have crossed capacity thresholds. If none of the systems have crossed a threshold, the widget will show an empty arc. Systems which have crossed the warning threshold are shown in yellow, and systems which have crossed the critical threshold are shown in red. Navigation from this widget will take the user to the Capacity Management page.

Select the Show detail control (>>) to display the **Capacity > Management** page.

Capacity Used widget

The **Capacity Used** widget shows ratio of space that is used to available space.

This widget shows the total percentage of capacity used. Since the widget does not represent a Health state, the text and color will always be a neutral state. The gauge will show blue to the ratio of the used capacity, and the text will always be blue. Navigation from this widget will take the user to the Capacity Management page.

Select the Show detail control (>>) to display the **Capacity > Management** page.

Replication Status widget

The **Replication Status** widget shows a summary for replication pairs and cascaded pairs.

This widget shows a count of systems which have replication issues. If there are no replication-related issues, the widget shows an empty arc. If there are systems with problems, then the widget shows the ratio of the issues. Navigation from this widget takes the user to either the Automatic or On-Demand Replication pages, depending on which type the widget was configured for.

Configuration options include setting the widget to monitor only Automatic or only On-Demand replications.

Select the Show detail control (>>) shows the **Replication > Automatic** page.

Lag Thresholds widget

The **Lag Thresholds** widget shows the count of replications with critical and warning levels, based on the Lag Threshold Policy.

This widget shows the count of pairs which have crossed lag thresholds. If none of the pairs have crossed the threshold, the widget shows an empty arc. Pairs which have crossed the warning threshold are shown in yellow, and pairs which have crossed the critical threshold are shown in red. If both warning and critical thresholds had been crossed for a replication pair, then the worst status (critical) takes precedence.

Select the Show detail control (>>) to display the Replication Automatic page(**Replication > Automatic**), where the list of all filtered replications is shown. The Lag Threshold Policy can be viewed or changed from here.

High Availability Readiness widget

The **High Availability Readiness** widget shows a status summary for all the HA systems in the inventory.

This widget shows the total number of HA systems, the number of HA systems that are not ready for failover, and the number of HA systems that are ready. If there are any HA systems that are not ready for failover, the gauge shows that fraction colored red. If all HA systems are available, the gauge shows all green.

Users can filter by systems, groups, properties, and rules. Filtering by systems shows only the HA systems available in the inventory.

Selecting the Show detail control (>>) takes you to the **Health > Status** page. If there are HA systems in the inventory, this navigation shows systems that are filtered by HA systems.

Clicking the gauge also goes to the **Health Status Page**, filtered by any HA systems that are not ready for failover. If all systems are ready for failover, going to the **Health Status Page** from the graphic shows a list of HA systems.

Cloud Health widget

The **Cloud Health** widget monitors the health from a cloud-enabled system's perspective.

A new **Cloud Health** option is available in the **Add Dashboard Widget** dialog box **Template** option dropdown. Selecting the **Cloud Health** option shows the preview image for the Cloud Health widget. This widget shows that the Cloud Tier health of Cloud extended systems in the inventory. Filters can be applied to the **Cloud Health** widget, similar to all the other Dashboard Widgets. Filter by System option for Cloud Health widget only shows a list of Cloud extended systems.

Monitoring Cloud Unit Health is done at the system level in DDMC. The Health Status view indicates the number of cloud enabled systems that are Active (green), Delete Pending and Disabled (yellow), and Error and Disconnected (red).

When the Cloud Tier of each of the Cloud extended systems that are registered with a DDMC is healthy, meaning the Cloud units on those systems are healthy, the Gauge is displayed in a Green color.

Clicking the Gauge (or the image within the widget or the Show Details (>>) button on the toolbar) goes to to the Health Status page, which is filtered by the complete list of the Cloud extended systems.

If a system has two cloud units, one in the Delete Pending and Disabled state and the other in the Disconnected state, the widget shows yellow.

When the Cloud Tier on some or all of the Cloud extended systems is not healthy, meaning one or more Cloud units on those systems are not healthy, the Gauge shows the fraction of the Cloud extended systems whose Cloud Tier is not healthy. If all five Cloud extended systems are Unhealthy, then the complete gauge is Red.

Clicking the Gauge (or the image within the widget or the Show Details (>>) button on the toolbar) goes to to the Health Status Page filtered by the Cloud Extended Systems that are Unhealthy.

If one Cloud Unit is healthy and one has errors, the widget should display **error** for the Cloud Tier and requires further troubleshooting to determine the source of the error and any remedial action that can be taken. The widget displays a gauge with the error proportion colored red and the remaining gray.

 **NOTE:** The worst state for the Cloud Units in a system takes precedence.

Users can filter by systems, groups, properties, and rules. Filtering by systems shows only the Cloud Extended systems available in the inventory.

Copying tabs

You can create a tab that contains the same widgets as an existing tab by copying that tab.

Steps

1. Select **Home > Dashboard**.
2. Select the **Add tab** control in the banner on the upper right.
3. In the **Add and Configure Dashboard Tabs** dialog, select the name of the tab to copy and then **COPY**.
4. In the text box, enter the new name for the tab (typing over "COPY OF ...").
5. If you want to change the number of columns, select the current number, and change it using the drop-down list.
6. If you want to change the placement of the new tab, use the **MOVE UP** or **MOVE DOWN** arrows.
7. Click **SAVE**.

Results

The new tab is displayed on the dashboard. You can open the widgets on the new tab to modify their properties.

Editing tabs

You can edit an existing tab by using the Filter icon on the upper right corner.

About this task

Click the Filter icon to:

- Filter by group
- Filter by property

- Filter by system
- Filter by rule
- Clear filter

Filtering tabs

Tabs can be filtered using the Filter icon on the upper right corner.

Click the Filter icon to:

- Filter by group
- Filter by property
- Filter by system
- Filter by rule
- Clear filter

Modifying widgets

You can modify widgets that were copied from a tab as a starting point for a new set; for example, you could change the filter properties to monitor a different group, set of systems, or rule.

To modify a widget, use the Edit widget icon on the widget's title bar, and change the name, settings (if available), and filtering.

 **NOTE:** You cannot change the widget type (as determined by the widget template) with the Edit function.

Organizing managed Data Domain or PowerProtect systems

As you organize and categorize each system, be aware that:

- Groups can be applied only to Data Domain or PowerProtect systems.
- Properties can be applied to systems, MTrees, and replication contexts.
- A default set of system properties (system model, DD OS version, and domain name) is automatically assigned when a system is added. *Custom* properties can be set. Data center properties can also be modified but not deleted.

After you have completed the initial setup for each system, you can assign values to properties or place a system in a group by selecting a system and clicking **Edit**.

Creating groups

Groups are ways to organize Data Domain or PowerProtect systems under a specific name, in a hierarchical structure created by the DDMC administrator.

About this task

Groups are helpful for performing searches. When used with filters, groups reduce the number of systems returned. Groups can contain other groups and systems. A group can belong to only one group, but a system can belong to many groups. You start by creating one or more root-groups at the Groups level, and then add sub-groups and systems.

 **NOTE:** Systems can be added at the root Groups node. However, group hierarchy structures cannot be changed. They must be deleted and re-created to change the structure.

Steps

1. Select **Administration > Groups**.
2. To add a group at the root level, click **+ ADD**.
3. Ensure only the "/" is in the Path box. Enter a name for the new group, and click **SAVE**.
The new group is now listed in the Groups panel.

- To add a sub-group to a group, select a group (which will be the *parent* group) from the Groups panel, click **+ ADD** (green plus sign), enter a name for the sub-group, and click **SAVE**.
The sub-group is nested under the parent group in the Groups panel.
- After a system has been added to DDMC, it can be added to a group. Select the target group from the Groups panel, and click **ADD** (green plus sign). In the **Add Group** dialog, select a system from the **Available Systems** panel, select **>** to move the system into the Systems in the Group panel, and click **SAVE**.
The system is displayed in the Group Details panel when the group is selected in the Groups panel. When a system resides in more than one group, you can hover the cursor on the Information control to display the group assignments.

Adding properties to systems and replication pairs

Properties provide information for classifying systems, and the data contained in Replication contexts, for searching, filtering, and organizing. For example, you could assign properties to help filter the list of Data Domain or PowerProtect systems in the **Inventory > Systems** page and narrow the scope of output that is produced by a dashboard widget or generated report. When a system is added to DDMC, a set of default administration properties (system model, DD OS version, domain name, and data center) is automatically added. You can add and assign other properties as needed.

Steps

- Select **Administration > Properties**.
- At top right, select one of the tabs (SYSTEM or REPLICATION), and click **ADD** (green plus sign).
- In the Add Property dialog box, type a name for the property, and select its operation type:
 - String** – Allows a string of up to 256 characters to be set when assigning the property, for example, you could name the property "Comments", and a user could enter "Waiting for Tom's response", "Not ready yet", etc.
 - Boolean** – Creates a condition where you can assign one of two values, for example, you could name the property "Restored?", and possible values could be "True" or "False", or "Yes" or "No".
 - Fixed-value String** – Lets you provide a name and specific values for the property, for example, "Department" could be the name, and "Finance", "Human Resources", "Marketing", etc., could be the values. Selecting the option **Allow multiple types** lets you assign more than one value.
- Click **ADD**.
- Assign values to the properties, as described in "Assigning Properties".

Related concepts

[Assigning properties](#) on page 38

[Displaying property information](#) on page 39

Related tasks

[Assigning system property values](#) on page 38

[Assigning replication property values](#) on page 38

[Displaying properties for an element](#) on page 39

[Finding elements by property value](#) on page 39

Adding (registering) systems to DDMC

Before you can manage a Data Domain or PowerProtect system in DDMC, you must add (register) it to the inventory. A single DDMC instance can have a maximum of 150 systems added. Groups of up to 20 systems can be registered at one time.

Steps

- Select **Inventory > Systems**.
- Click **ADD** (green plus sign). Type the following for the first system, then select **Add** to continue adding systems (up to 20 systems total). Ensure the box next to the system being added is checked.
 - Select **System** or **HA system**.
 - Host name** (required) – Type the fully qualified hostname (use alphanumeric characters, dashes, periods, and underscores) or IP address. Ensure that the hostname and the DNS name for the system match; a mismatch may cause problems with backup software.

NOTE: For HA systems, specify the floating hostname, otherwise the Add operation fails.

- **Sysadmin password** (required) – Type the sysadmin password that is used on the Data Domain or PowerProtect system (required).
- **Proxy Firewalls** (optional) – Type the inbound and outbound proxy hostname (or IP address) and port number to be used by the firewall. If this option is selected, and you do not change the port number, the default (3009) is used. If you do change it, the port number must be between 1 and 65535. The default port settings let DDMC communicate with the system. If the ports have been changed on the firewall or the system, they should also be updated here.

NOTE:

- Proxy firewalls are not supported for HA systems, so this section is not editable when adding an HA system.
- For more detailed information, see the section, [Inbound and outbound proxy host names and port numbers used by the firewall](#) on page 35.

- **Certificate** (optional) – Check certificate information by clicking in the associated cells. The Subject name in the DDMC CA certificate should match the DDMC hostname, or SSL fails the host verification.

NOTE: For environments that use self-signed SHA-256 certificates, the certificates must be regenerated manually after the [upgrade process](#) is complete, a trust must be reestablished with external systems that connect to the system.

- **Progress** – Shows the percentage that is completed as the system is being added.
- **Takeover managed system** – Select this checkbox if the system is managed by another DDMC. The system becomes unmanaged but not removed from the other DDMC.

3. Click **REGISTER** to continue.

Results

A progress bar displays on the page showing the progress of the initial data synchronization for the newly added systems. Also, job progress details can be tracked on the **Health > Jobs** page.

NOTE: If there is a failure, select **Get failure reason** on the progress bar. After correcting the failure reason issue, click **REGISTER** to re-register again.

After a system is added to DDMC, all historical information for that system is copied to DDMC. From that point on, whenever operational data changes on that system, the system notifies DDMC, which immediately polls the system to receive that new information.

Common Causes of Errors While Adding Systems

The following checklist may help you resolve some errors that can occur when trying to add a system to DDMC:

- Ensure that the system is online. A system *must be online* to be added to DDMC.
- If you specified a port number in the proxy firewall settings, ensure it is correct.
- Ensure that there are no networking issues preventing communication between the DDMC and the system.
- If you specified a hostname for the system, ensure that the hostname can be resolved in the namespace (DNS or host list).
- Ensure the password that is entered for the system is correct.
- Ensure that the DD OS version of the system is supported by the current version of DDMC.
- Ensure that the system is not already managed by another DDMC. To resolve this issue, you can either delete the system from the original DDMC or select the **Takeover managed system** checkbox. The system is added to the new DDMC, but the system's status will be changed to *unmanaged* on the original DDMC, and data collection will be suspended for that system.
- For HA systems, ensure:
 - The specified hostname was not the hostname of the standby node.
 - The HA system is not in degraded mode.
 - Both of the nodes are up.

Configuration Templates

Configuration Templates allow a DDMC administrator to create a template for configuring a Data Domain or PowerProtect system.

This function allows:

- The same configuration to be applied to multiple devices.

- A known valid and preferred configuration from a DD System to use as a standard template.
- Monitoring of multiple systems for configuration compliance and audit changes that are made by whom and when.

NOTE: A Configuration Template is based on configuration from a source system and cannot be created from scratch in DDMC.

Template details can be viewed clicking the Details button in the table row. For additional configuration details, click **View Configuration Details** in the details panel on the right side.

Create Configuration Template

1. Select **Inventory > Configuration Templates**.
2. Click **Create**.
3. Name the template (required).
4. Select the source configuration system from a list of existing systems managed by DDMC.

NOTE: The source system must be online and reachable.

5. Select or clear any feature or subfeature.
6. Click **Create Template**.

Delete Configuration Template

1. Select **Inventory > Configuration Templates**.
2. Select the Configuration Template to be deleted.
3. Click **Delete**.
4. In **Delete Templates** dialog, click **YES** to confirm deletion.

Apply Configuration Template

NOTE: Only online systems will be shown in the Available Systems list to apply a template.

1. Select **Inventory > Configuration Templates**.
2. Select the Configuration Template to be applied.
3. Click **Apply**.
4. Search in Select Systems and select the system(s) that the template will be applied to from the Available Systems list.
5. Click **Add**.
6. Click **Next**.
7. Click **Apply**.

Inbound and outbound proxy host names and port numbers used by the firewall

The inbound and outbound proxy host names (or IP addresses) and port numbers for a firewall must be set if the connection between DDMC and the Data Domain or PowerProtect system is through a proxy.

NOTE: This section is disabled when adding HA systems.

NOTE: In DDMC, ports 8009 and 8080 are restricted to localhost only and are inaccessible from outside. DDMC is accessed by default HTTP port 80 or, if SSL is enabled, by default HTTPS port 443.

The terms *inbound* and *outbound* are from the perspective of DDMC. *Inbound* means from the system to DDMC, and *outbound* means from DDMC to the system.

Starting with the simplest situation (direct connection) for explanation, here are some scenarios and how you would set up the inbound and outbound proxy firewall host names (or IP addresses) and port numbers.

DDMC connecting directly to a system (simple case)

In the simplest case of connecting DDMC to a Data Domain or PowerProtect system, the system can resolve "ddmc.myco.com" to 1.1.1.1, and DDMC can resolve "ddr.myco.com" to 1.1.1.2.



Figure 3. Simple case: DDMC connecting directly to a system

In this simplest case, it is assumed that:

- DDMC can connect to the system using TCP.
- The system is similarly able to connect to DDMC using TCP.
- DDMC, by default, tries to translate the hostname of a system (that is, the name that is returned using `net show hostname` or the name that you see in the DD System Manager) to an IP address using DNS or a host file.
- The system similarly tries to translate the DDMC hostname to an IP address using DNS or a host file.
- DDMC connects to TCP port 3009 on the system, and the system connects to TCP port 3009 on DDMC.

A system with multiple network interfaces

When a system has *multiple network interfaces*, you need control of the specific interface that is used by DDMC.

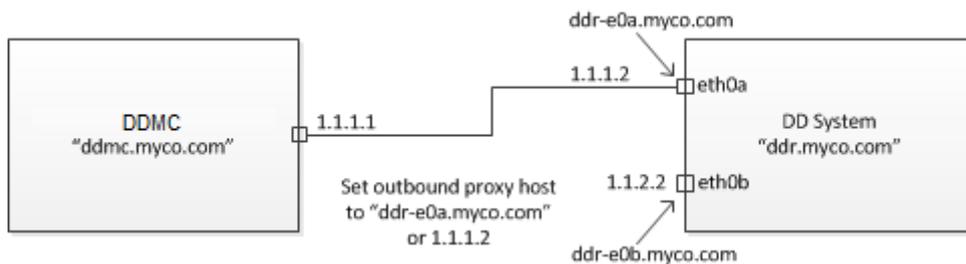


Figure 4. System with multiple network interfaces

In this case, the system hostname probably does *not* translate to the IP address of the wanted network interface. To direct DDMC to the wanted interface, you must set the outbound proxy hostname (or IP address) to a DNS name or the IP address of the wanted interface. It is not necessary to set the inbound proxy hostname or port number.

NAT firewall between DDMC and system

When a NAT (network address translation) firewall exists between DDMC and a Data Domain system, the firewall is configured so that when you connect to a port on the firewall, the firewall proxies that connection to an IP address and port number on the destination system. The IP address to which DDMC connects does not match any IP address on the system itself. Port numbers may be re-mapped as well. To connect to a system, you would connect to a port other than 3009 on the proxy.

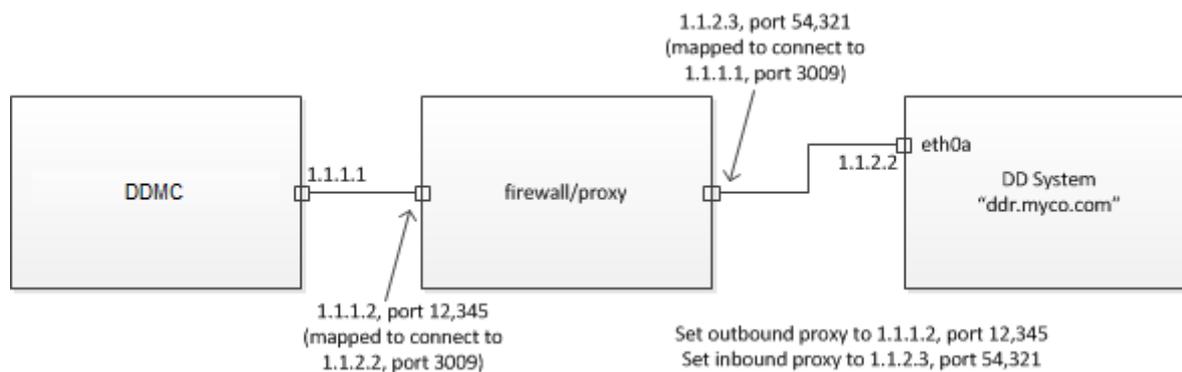


Figure 5. NAT firewall between DDMC and system

In this case, when DDMC wants to connect to port 3009 on the system, DDMC must try to connect to port 12,345 on the firewall. Conversely, when the Data Domain system wants to connect to port 3009 on DDMC, the Data Domain system must try to connect to port 54,321 on the other side of the firewall.

To configure this, set the outbound proxy hostname to 1.1.1.2 and the outbound proxy port number to 12,345. Set the inbound proxy hostname to 1.1.2.3 and the inbound proxy port number to 54,321. The rule is that the outbound hostname and port number are the addresses to which DDMC should try to connect when it wants a connection to port 3009 on the Data Domain system. The inbound proxy hostname and port number are the addresses to which the Data Domain system should connect when it wants a connection to port 3009 on DDMC.

Avoiding the addition of host names to peer's DNS server or /etc/hosts file

There may be situations in which you do not want to add the hostname of the DDMC, or the hostname of the system, or both, to their peer's DNS server(s) or to their peer's /etc/hosts file.

In these situations, depending on the host name(s) you do not want to add, you can instead specify the IP address of DDMC in the inbound proxy hostname field and/or the IP address of the system in the outbound proxy hostname field.

Editing Data Domain or PowerProtect system settings

After Data Domain or PowerProtect systems have been added to DDMC, you can edit their configuration settings, properties, group assignments, and thresholds.

Steps

1. Select **Inventory > Systems**.
2. Select one or more systems and then EDIT (yellow pencil).
3. In the **Edit System** dialog, choose any or all tabs to make changes (select **APPLY**, or change tabs to save the new settings and continue reconfiguration). If you selected more than one system, only the Properties and Thresholds tabs are available.
 - **Configuration** lets you edit the inbound and outbound proxy hostname (or IP address) and port number to be used by the firewall. If this option is selected, and you do not change the port number, the default (3009) is used. If you do change it, the port number must be between 1 and 65535. The default port settings let DDMC communicate with the system. If the ports have been changed on the firewall or the system, they should also be updated here.

NOTE: Configuration is not displayed for HA systems.

NOTE: For more detailed information, see the previous section, [Inbound and outbound proxy host names and port numbers used by the firewall](#) on page 35.
 - **Properties** lets you edit information for classifying systems, and the data contained in MTrees and Replication contexts, for searching, filtering, and organizing. If you selected more than one system, and there are different values for that property on the different systems, the field will show *Mixed values*. If you change the value, all systems will receive the new value. There are default and user-created (**Administration > Properties > System**) properties. The default properties of Model, operating system, and Domain Name are not editable. Data Center is a "hybrid" fixed-value string-type property. Because it is a default system property, it cannot be deleted, but its values can be edited and set for a system.

- **Groups** let you organize systems under a specific name, in a hierarchical structure that is created by the DDMC administrator, which is helpful for searches. You can add or remove group assignments, and select or clear group assignments for the system. Any number of groups and subgroups can be selected.
- **Thresholds** indicate the system warning and critical capacity thresholds and are shown on capacity views and in reports. Use the slider to specify thresholds as a percentage of total capacity. When editing multiple systems with mixed warning thresholds, the initial warning value is zero. When editing multiple systems with mixed critical thresholds, the initial critical value is 100. If you change the value, all systems will receive the new value.

4. Select **OK** to save and exit system reconfiguration.

Assigning properties

The procedure to assign a property varies, depending on where the property is used: system or replication.

Related tasks

[Adding properties to systems and replication pairs](#) on page 33

Assigning system property values

After you add a property to a Data Domain or PowerProtect system (**Administration > Properties > System**), you can assign values to that property.

Steps

1. Select **Inventory > Systems**.
2. Select one or more systems.
3. Select **EDIT** (yellow pencil), and in the **Edit System** dialog box, select the **PROPERTIES** tab.
Data Center is the default property that should appear when adding a system.
4. For each property listed, assign a value. If you selected more than one system, and the systems have different values for that property, the field shows *Mixed values*. If you change the value, all systems receive the new value. An **Undo** control is provided for undoing the setting, and a **More Details** control shows the saved values for each selected system. For properties that were created as a:
 - String – Type the text that will be displayed as the value.
 - Boolean – Select one of the two values from the drop-down list.
 - Fixed-value string (and multi-value) – Select the value from the drop-down list.
5. Click **OK** to set the values.

Related tasks

[Assigning replication property values](#) on page 38

[Adding properties to systems and replication pairs](#) on page 33

Assigning replication property values

After you add a replication pairs property (**Administration > Properties > Replication**), you can assign values to that property.

Steps

1. Select **Replication > Automatic**.
2. Select a replication pair.
3. Select **ASSIGN PROPERTIES** and set a value. For properties that were created as a:
 - String – Enter the text that will be displayed as the value.
 - Boolean – Select one of the two values from the drop-down list.
 - Fixed value string (and multi-value) – Select the value from the drop-down list.

4. Click **ASSIGN** to set the values.
5. To see values that are assigned to replication contexts, you can add this property as a column in the replication table on the Automatic replications page:
 - a. Select the Show Columns icon.
 - b. Select the checkbox of the property from the list.
 - c. You will see the name of the property as the column title, and any value that is assigned to a context will appear in the cell.

Related tasks

[Assigning system property values](#) on page 38

[Adding properties to systems and replication pairs](#) on page 33

Displaying property information

Assigned property values can be displayed either by selecting an element (such as a Data Domain or PowerProtect system) and displaying all properties that are assigned to it, or by selecting a property and displaying all assigned elements.

Related tasks

[Adding properties to systems and replication pairs](#) on page 33

Displaying properties for an element

How you display properties for an element depends on the type of element: systems or replication pairs.

Steps

- **Systems** – Select **Inventory > Systems**, and select a Data Domain or PowerProtect system. All properties assigned to that system are displayed in the Properties panel.
 -  **NOTE:** You can also display properties by selecting the "gear" control in the systems banner. When you select one or more properties from the list of configured properties, a column for that property is added to the table. To hide the property, clear the property from the list. Some properties may not be removed from the table, so they will not display in the list of configured properties under the gear control.
- **Replication** – Select **Replication > Automatic**, select a replication pair, and select **Pair Details**. Any properties assigned to the replication pair are displayed in the Properties panel.

Related tasks

[Finding elements by property value](#) on page 39

[Adding properties to systems and replication pairs](#) on page 33

Finding elements by property value

You can also find elements by looking at all of the assigned property values.

Steps

1. Select **Administration > Properties**, and select the property type (**SYSTEM** or **REPLICATION**). The table shows all of the properties that have been created. Selecting a property displays its assigned values in the panel at the right.
2. To display where the property is assigned, select a property, and select the icon on the right side of the Key column. In the Property Assignment dialog, you can see the property type, the element where it is assigned, and the property values.

Related tasks

[Displaying properties for an element](#) on page 39

Managing groups

Although group creation and modification can be performed only by the DDMC system administrator, any user can apply group designations to their Data Domain or PowerProtect systems and can see the complete group structure, although role-based access control (RBAC) permissions control the systems that are displayed for each user.

Any permissions that are applied to a group affect all systems in that group. A lock image is added to the groups folder icon when permissions are directly applied to that group.

Use the **Administration > Groups** page to perform group management:

- Use **ADD** to create groups or to add systems to existing groups.
 - Use **DELETE** to remove systems from the group-level organization. (You cannot use delete to remove systems from a group. But you can edit the group, and remove systems by selecting them in the right panel and selecting the left-pointing arrow)
 - Use **EDIT** on a selected group to modify the presence of systems within that group or the name of the group.
-  **NOTE:** Groups cannot be dragged and dropped into a different location; they must be changed with the **Edit** function.

Managing replication lag threshold policies

Replication lag threshold policies warn you when replication pairs do not complete replication within a set amount of time.

About this task

By assigning a replication lag threshold policy, you are assured that notifications will be displayed in the **Replication > Automatic** page and the **Replication Lag Status** widget when the replication has not completed within the time periods you have set for Warning and Critical levels.

The default policy level for Warning is 24 hours, and the default for Critical is 48 hours.

Replication lag threshold policies can be created only for MTree, collection, and directory replication. Lag threshold policies for On-Demand replications are not supported.

Steps

1. Select **Replication > Automatic**.
2. Select one or more replication pairs from the table.
3. To create a policy, select **LAG THRESHOLD POLICY** (or right-click the pair, and select the option).
 - a. In the **Assign Lag Threshold Policy** dialog, from the Threshold policy menu, select **Create a new policy**.
 - b. In the **Manage Lag Threshold Policies** dialog, select **ADD**.
 - c. In the text box, enter the policy name, and use the slider controls to set the threshold points for the Warning and Critical lag levels.
 - d. Click **SAVE**.
4. Back in the Lag Threshold Policy dialog, select a policy from the Threshold Policy menu, and click **ASSIGN**.

Results

The policy is applied to the selected replication(s). The assigned policy name is displayed in the table in the Threshold Policy column.

To modify or destroy a policy, select **Manage Lag Threshold Policies** (or right-click the pair and select the option). In the Manage Lag Threshold Policies dialog, select a policy from the list, and select **Edit** or **Delete**. If a deleted policy was assigned anywhere, it is replaced with the Default policy. Select **Save** to exit.

 **NOTE:** The Default policy cannot be renamed or deleted, but it can be modified.

Working with filters

Filters are used to selectively define the output of a DDMC function. For example, filters can be used to define the scope of elements that display on a page, tailor the output of a report, or target the Data Domain or PowerProtect systems to be monitored for Dashboard widgets. The **Filter** (funnel-shaped) control appears on pages and dialogs whenever a filter can be used.

About this task

The drop-down menu on the **Filter** control allows you to select the groups, properties, systems, or rules to be used for filtering. When a filter is active on a page, the **Filter** control is selected. Filtering can be switched on or off using the **Filter** control as a toggle.

The **Filter by rule** option lets you create custom rules that can be saved for reuse or run in the current location. The rule can be built using any of the standard filter criteria (groups, properties, and systems), along with any existing properties or groups that have been created. Controls for logic (is, is not, contains, does not contain, so forth) are provided, and statements can be inclusive or selective.

 **NOTE:** Global Filter is only available in **Classic view** and is not supported in the **Cloud** tab.

To create a custom filter rule:

Steps

1. From the **Filter** drop-down menu, select **Filter by rule**.
2. In the Filter by Rule dialog, provide a name for the filter.
3. Using the selection menus in the **Match the following** area, create the criteria for your rule. The criteria consists of one or more statements.

Create the first statement by selecting an object from the first menu (System, Group, Model, OS, Domain Name, etc.) and a logic condition (contains, does not contain, is, is not, etc.), then the target (text you input or a menu selection, based on the previous selections). For example, a statement could be "Model is DD880".
4. If needed, add more statements with the **Add row (+)** control, or add conditions to the rule using the **Block (...)** control, which adds the choice of **All** or **Any** to the Match the following area), and create additional statements.
5. Select the **Save** (disk) control to make this filter available from the **Filter** menu list or select **Filter** to run the filter once and exit.
6. To remove the filter and return to unfiltered content, select **Clear filter** from the **Filter** menu.

 **NOTE:** The filter may still be available with the **Recent filters** option on the **Filter** control list.

Related concepts

[Viewing DDMC page elements](#) on page 27

[Global controls and icons](#) on page 123

[Dashboard controls](#) on page 125

Monitoring Systems

Topics:

- How DDMC helps you monitor Data Domain and PowerProtect systems
- Data retention policy for DDMC
- Space projection algorithm for DDMC
- Performing daily monitoring
- Monitoring capacity
- Checking the System Details lightbox
- Monitoring replication
- Monitoring status with reports

How DDMC helps you monitor Data Domain and PowerProtect systems

The monitoring tools of DDMC let you examine a wide array of operational information about managed systems.

After a Data Domain or PowerProtect system is added to DDMC, all historical information for that system is copied to DDMC.

When operational data changes on a system, the system notifies DDMC, which immediately polls the system to get the latest operational data.

DDMC monitoring tools draw on this data for current and historical reporting and for creating trend projections.

DDMC monitoring tools are highly visual – using charts, graphs, and color coding to help you interpret essential data points and easily notice alerts for critical markers.

DDMC monitoring tools help you focus on areas of interest. They can show mile-high status checks of all managed systems and check a specific group of systems, as well as drill-down to check the health or operational history of a single system's components. For capacity monitoring, you can easily check current operation and historical data and perform capacity predictions based on usage trends.

Using the filtering and grouping options that are provided on monitoring pages, DDMC lets you easily shape your data presentation so you can focus on viewing just the information you need.

In addition to data provided on the interface, you can generate reports to compile operational data that can be exported. Reports can be generated ad hoc or scheduled and emailed to a list of interested parties.

Data retention policy for DDMC

DDMC maintains up to ten years of performance and capacity measurements for the Data Domain and PowerProtect systems it is monitoring. Data from the systems are consolidated into hourly sample points, generally collected at 30 minutes past the hour. The hourly samples are consolidated into daily samples, where a day is considered to run from *Noon to Noon*. Daily samples are further consolidated into weekly samples, where a week begins on Sunday.

To reduce the amount of space needed to store this historical data, DDMC periodically discards older samples. The number of samples retained depends on the nature of the data and whether the sample is hourly, daily, or weekly data. The following table shows the length of time that DDMC retains each sample.

Table 8. Data retention policy for DDMC

type of data	keep hourly samples for	keep daily samples for	keep weekly samples for
Collection space usage	3 months	1 year	10 years

Table 8. Data retention policy for DDMC (continued)

type of data	keep hourly samples for	keep daily samples for	keep weekly samples for
MTree space used	1 month	3 months	10 years
Automatic replication (bytes transferred and lag)	1 month	3 months	10 years
On-demand replication (number of files and bytes transferred)	3 months	1 year	10 years
Performance (CPU and network)	1 month	1 year	none created or retained

Finally, DDMC retains up to 2,000 historical alerts from each Data Domain system being monitored.

Space projection algorithm for DDMC

DDMC uses a sophisticated algorithm to project growth in space usage and to predict when a Data Domain or PowerProtect system will run out of space. This algorithm was developed and verified using years of autosupport reports and should be accurate.

For this algorithm, DDMC uses a *seven-day moving average* instead of actual measured values. This smooths out the effects of file system cleaning and other activities that repeat every week (for example, deleting an old full backup and creating a one every weekend).

The goal of this algorithm is to compute a linear projection of space growth using an optimal set of recent data points. The data history is scanned to find the projection with the best fit, that is, the regression with the highest R^2 value.

The R^2 value is a measure of how close the regression fits the actual measurements. A value of "1" means that the fit was perfect. A value of "0" means there was no fit at all. A value of "0.8" means that DDMC found a projection that matches the measurements closely enough to be meaningful and not misleading.

After the best fit is determined, the projection must pass the following validation tests to ensure that the prediction is accurate:

1. DDMC must have at least 15 days of historical data.
2. The regression R^2 value must be at least 0.8 or higher.
3. The slope of the regression must be positive (that is, space usage is growing, not shrinking).
4. Time-to-full must be less than 10 years in the future.
5. The system must be at least 10% full.
6. The most recent data sample must be within 5% of the projection.

Combining all these validation criteria accounts for typical system usage behavior, such as space becoming free after a cleaning cycle, jumps in usage as new backup loads are stored on the system, and space becoming free when backups are deleted.

Performing daily monitoring

Using DDMC to perform daily monitoring of your site lets you check for unusual activity before it becomes a serious problem.

You should perform the following tasks *at least daily* to get an overview of the operational status of your Data Domain or PowerProtect systems and data replication.

Checking dashboard status widgets

The **Home > Dashboard** widgets (Health Status, Active Alerts, Capacity Thresholds, Capacity Used, Replication Status, Lag Thresholds, High Availability Readiness, and Cloud Health) provide an overview of key performance indicators for your monitored Data Domain or PowerProtect systems.

By default, one tab is provided named **All Systems** that is populated with one of each type of widget.

The graphs, dials, and color-coded alerts make it easy to spot system operational problems. Many components on the widgets provide a link to a full-featured page for the function so you can drill-down to see complete information.

If any of its monitored systems are not reachable (because they are Offline, Not Responding, Unsupported OS version, Not Transmitting, or Unmanaged), a **Status** button appears at the upper right corner of a widget (except for Active Alerts).

Selecting this button shows the count of systems with connection issues. Selecting the **Show Health Status** link opens the **Health > Status** page, where a list of these systems is displayed.

Widget templates for commonly used monitoring functions can be used to create widgets for all managed systems or filtered by a set of criteria such as groups, properties, systems, or rules.

After they have been created, you can drag widgets around the dashboard to improve their organization. A widget or a tab with several widgets can be copied and modified to create additional widgets.

The size of the dashboard can switch between full screen and normal view.

Checking system capacity

The system capacity widgets help you to spot shortfalls in overall managed storage capacity and monitor managed system storage usage.

Capacity Thresholds

The Capacity Thresholds widget displays systems that have crossed warning or critical storage capacity levels.

Capacity Used

The Capacity Used widget lets you monitor aggregate totals of storage levels for all Data Domain and PowerProtect systems it is configured to manage. This widget monitors the total storage capacity of all systems (for space that is used and available) or a selected group if a filter is set.

Checking replication progress

The replication widgets provide replication status and issues.

Replication Status

The Replication Status widget highlights replications with performance problems for the widget's monitored systems.

Lag Thresholds

The Lag Thresholds widget identifies replication pairs which are not replicating data to the destination fast enough and shows the count of replication pairs which have crossed the Critical, Warning, and Normal threshold levels, based on the assigned policies. This widget identifies these pairs, the duration of the lag time and whether it is improving.

Checking health and alerts

The Dashboard health status and alerts widgets highlight systems that are reporting major reachability or operational problems. And if there are problems, the widgets provide drill-down links to system details.

Health Status

The Health Status widget highlights unreachable systems and systems experiencing issues with file system and replication operations, alerts, and data transmission protocols. The widgets show All Normal (green) or show a count of systems exhibiting issues.

Clicking on the gauge navigates to the **Health Status** page, filtered by the systems in Not Healthy status, if any.

Active Alerts

The Active Alerts widget displays a tally of systems with outstanding alerts for Emergency & Alert, Critical & Error, and Warning, using a colored gauge and a rolled up count of Alerts for each system. The worst status takes precedence.

Clicking on the gauge takes you to the Alerts page, filtered by the widget's configured filters .

Checking alert notifications

For new, unacknowledged alerts on systems you are authorized to manage, always check the "Notification Area," located in the lower left of the Status Bar (the bottom border of the DDMC window).

This Notification Area is not constrained by filter settings that are active, that is, it displays notifications of alerts for all of the systems you are authorized to manage.

The "New Alerts" area shows the current unacknowledged Emergency, Error, and Warning level alerts. Click anywhere in the New Alerts area to display a pop-up reporting the severity, system name, and class of the new alert. After the pop-up has been displayed, the alerts notification is removed from the Alerts Notification area.

To see the alert details, select the "Show me these alerts" link to open the **Health > Alerts** page, where the table is filtered to show only the new alerts.

Checking health status

The **Health > Status** page displays information about potential operational problems, such as connection status, replication status, and alerts.

The Systems/Groups/Tenants icons at the upper right let you show all Data Domain and PowerProtect systems and systems organized by group or Tenant assignment.

 **NOTE:** Secure Multi-tenancy functionality requires systems running DD OS 5.5 or later.

LED colors indicate:

- Red – error or problem
- Yellow – error or warning
- Green – normal operation
- Gray – disabled components
- Gray "Empty Socket" – non-licensed components

 **NOTE:** If a system is unreachable – but not disabled or non-licensed – the last known state of the LED is displayed. An unreachable, or not transmitting system, may still be operational for backups, restore, and replication, but it is not communicating with DDMC.

For all three views:

- Hover the cursor over a gray LED in the Replication column to get a link to the Replication Overview, showing the pairs related to this system or Tenant Unit.
- Hover the cursor over a red/yellow LED in the Alerts column to get a link to open the Alerts page.
- Use the Sort Ascending option for the Connection Status column to find connection problems on systems.
- If the File System is destroyed or disabled, a red LED is displayed. As a result of this non-activity, Protocols and Replication are affected and display a red LED as well.

For the Systems or Groups views:

- Hover the cursor over an "empty socket" LED to get a link to launch DD System Manager.
- The System Details control (upper-left) launches the System Details Lightbox for the selected system.

For the Tenants view:

- When a system is offline, the Tenant Units in that system become offline as well, and the Tenant Unit offline icon is displayed in the Tenant Unit tree.
- Unmanaged Tenant Units, as well as MTrees and Storage Units that do not belong to a Tenant Unit, are not displayed.
- Only Tenants and Tenant Units that belong to the current user are displayed.
- The Tenant Unit Details control (upper-left) launches the Tenant Unit Details Lightbox for the selected Tenant Unit.

Checking health alerts

In addition to checking Health Status for operational problems, also check the **Health > Alerts** page. Be sure to watch for new or repeating alerts.

Use the Systems/Tenants icons at the upper right of the page to switch page content to show all Data Domain and PowerProtect systems or systems that are organized by tenant assignment.

When you select the Tenants icon, note the following:

- The Tenant Unit Details control (upper left) launches the Tenant Unit Details Lightbox.
- A special "all" Tenant Unit alert is applied to all Tenant Units in the system.

 **NOTE:** Secure Multi-Tenancy functionality requires systems running DD OS 5.5 or later.

The page banner provides summaries of the total number of alerts: those that are errors and above, and those that are warnings.

At the upper right, you can select the Active Alerts or All Alerts tab, depending on what you need to view. Many, but not all, alerts remain active until manually cleared.

The Date range filters (Last 12 hours, Last 24 hours, Last 7 days, Last 30 days, All active alerts, and Custom). let you narrow or expand the focus of alert scoping or go back to a specific point in time.

The column controls sort the alert list by Severity, System Name, Post Time, Class, Message, and Object ID. The System Name column includes a filter for entering system name text.

Selecting an alert in the table expands to show descriptive information about the alert. To see a summary of the alert's history, select the **More Details** link to see a list of every occurrence of the alert at the site.

To investigate or resolve an alert on a system, open the DD System Manager by double-clicking the alert in the table, or use the **Launch DD System Manager** control, which is enabled when a system alert is selected.

 **NOTE:** For additional information about specific alerts, see the Error Message Catalog on the online support site.

Checking health jobs

In addition to checking Health Status for operational problems, also check the **Health > Jobs** page. This page displays information about jobs (also called tasks) that have been initiated from DDMC, including jobs still in progress and jobs that have completed, whether successfully or not. Details of a task, including its subtask status, are shown for a selected task in the Details panel.

You can filter jobs by Failed, In-progress, and/or Completed.

You can select a job from the main list and expand the steps to see sub-steps up to 10 levels deep.

Tasks can run on the DDMC alone or can run on the DDMC and a Data Domain and PowerProtect system. For example, the Report Generation task runs solely on DDMC. Other tasks, like Upgrade, run mostly on the system, but a skeleton process on DDMC tracks the task's progress. And still other tasks run mostly on DDMC (such as Adding Systems), but have subtasks that run on the system. Tasks that run on DD System Manager are not shown in the Jobs list – only those tasks that are initiated from DDMC are shown.

The displayed list of tasks is dependent on the role:

- A person with a *user* or *limited-admin* role on a system or DDMC sees only the tasks that they initiated on that system or DDMC.
- An *admin* on a system or DDMC sees all jobs on that system and DDMC.

Monitoring capacity

The Capacity pages display information about storage utilization and allows for toggling between managed systems, Cloud Tier, and MTrees. Current and historical space consumption, as well as estimate projected near-term future storage needs, can be monitored from here.

Checking system capacity and disk space usage

The **Capacity > Management** page displays storage usage amounts for monitored Data Domain systems (default), data in the cloud, or their MTrees.

NOTE: This guide assumes that you are familiar with capacity terms, as introduced in the *Data Domain Operating System Administration Guide*. See that guide or the DD System Manager Online Help for explanations of these terms.

The Cloud, System, and MTree tabs at the upper right of the page allow for a choice in how to display data. The **System** tab has two views: **Systems** and **Groups**, and the **MTree** tab has views for **Systems** and **Tenants**.

Physical capacity (PCM) for MTrees, Tenants, and Tenant Units can be measured and is described in more detail in the next section, [Measuring Physical Capacity \(PCM\)](#).

Capacity Management/Systems View is the default view and can:

- Identify systems as targets for new back ups, replication, and migration
- View the amount of data that is written during a particular timeframe, such as a back-up cycle, and determine how much it has been compressed
- Identify systems that have deviated from their norm for compression ratio, and so forth
- Monitor the capacity of logically grouped or single systems to track usage and identify systems that are using capacity too quickly
- Identify systems that have used all their storage space
- For Extended Retention-enabled systems, identify how much space is available and used on the Archive and Active tiers, and how well it is compressed
- Identify when garbage collection runs and how much space is reclaimed
- Sort the Warning and Critical Capacity Thresholds columns by ascending/descending controls and can be filtered by an entered value (greater, lesser, or equal to entered value).

Space usage amounts are shown for the current time in the **Capacity Usage**.

NOTE: The Space Usage amounts may not exactly match capacity totals that are reported by DD System Manager. Because of the polling delay of up to an hour, DD Management Center reporting will always lag. This is especially true if there is a lot of churn on the monitored system. The discrepancy will be more visible, and there is a possibility that DD Management Center may never catch up with DD System Manager capacity totals.

Capacity Management/Mtree/View by tenant can:

- Type a list of comma-separated strings to filter the Tenant Unit column.
- Sort MTrees within a Tenant Unit.
- Monitor the capacity of logically grouped or single systems to track usage and identify systems that are using capacity too quickly

In the **Capacity Usage** section:

- When a Tenant Unit is selected, the information is aggregated based on all MTrees within that Tenant Unit.
- When a Tenant is selected, the information is aggregated based on all MTrees within all Tenant Units pertaining to that Tenant.
- The last row shows aggregated totals.

In the **Measured Physical Capacity** section, note that **Job State** can have one of the following five values:

- Unsupported (Data Domain system does not support PCM features)
- Completed (latest job successful)
- Failed
- In-progress
- None (PCM is supported, but no jobs run)

In the **Charts** area, the **Space Usage**, **Consumption**, and **Data Written** information and can be seen by selecting each in a drop-down list. If there are connected systems with Cloud Tier or Retention Tier, tabs are shown as Retention (for both Cloud Tier and Retention Tier) and Total. New charts for the Cloud Tier are also available.

- Systems that are consuming space at a rate significantly greater or less than their historical norm
- Total capacity, amount that is consumed, and compression ratio (aggregate) for a group of systems
- Data ingest rate for a group of systems, for example, the total data ingest rate for the last 24 hours
- Systems that are out of space or critically low on space or have used all of their storage space
- The amount of data that was backed up the previous night (24 hour period), and the compression ratio for a group of systems
- The last time that garbage collection was run and how much space was reclaimed
- Select multiple systems and see aggregated information

Capacity Management > Cloud view can:

- Monitor the active tier and cloud tier capacity residing on different cloud providers
- Give an overview of the data distribution between on-premises data centers and the different cloud providers
- List which Mtrees are associated with a certain Cloud provider

Measuring physical capacity

Physical capacity measurement (PCM) provides space usage information for a subset of storage space for MTrees, Tenant Units, and Tenants.

PCM measures the physical capacity consumed by a subset of files within the file system, based on how the files in the subset deduplicate with other files in the subset. In other words, it measures the physical capacity that would be consumed on a Data Domain or PowerProtect system by a set of files, if that set of files were the only files on the system. This is a *point in time* measurement, based on when the measurement is requested.

You can specify the file system subset to measure in several ways: as an MTree, a Tenant Unit (all files within a Tenant Unit), or a Tenant (all files within a Tenant). Since a Tenant can span systems, in this case DDMC measures and reports the physical capacity consumed by the Tenant on each system.

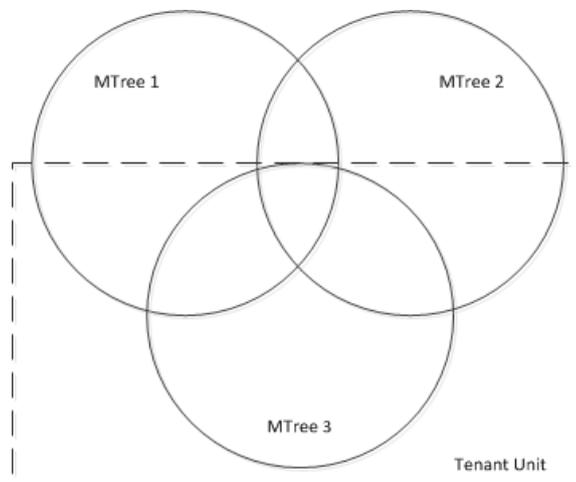
The results of PCM jobs are retained for no more than one result per hour for the last 90 days, then no more than one per day for the last year, and then no more than one per week for the last 10 years.

Managing measurement schedules for physical capacity

You can management measurement schedules for physical capacity using the Manage Measurement Schedules dialog.

About this task

NOTE: You cannot directly *add up* Physical Capacity Measurements because a certain amount of *sharing* occurs between MTrees, so any totals generated can often be misleading. In the following picture, the Tenant Unit's information is stored on three MTrees, but there is sharing among those MTrees, so the actual total would be less than simply adding up the space used by the Tenant Unit.



Schedules may be consolidated on multiple Data Domain and PowerProtect systems, as follows:

- If two or more schedules have the same name, type, and schedule (for example, "every Monday at 7 AM"), DDMC displays one schedule configured on different systems.
- If two schedules have the same name, but different types and/or different scheduled times, DDMC displays two schedules.
- If a schedule is *Disabled* on one system, but *Enabled* on another, DDMC displays one schedule.

 **NOTE:** Refresh can take up to one hour if these changes are made through the command-line interface (CLI).

Steps

1. Select **Capacity > Utilization > MTree tab > Physical Capacity Measurement menu > Schedules**
2. In the Manage Measurement Schedules dialog, you can add a new schedule, edit an existing schedule, or delete a schedule.
3. For existing schedules, expand the arrow at the left to display the entities that belong to the selected schedule:
 - **Schedule** shows the current schedule, such as *Daily at 12:00*.
 - **Type** can be *MTree*, *Tenant Unit*, or *Tenant*.
 - **Status** indicates whether the schedule is *Enabled* or *Disabled*. If disabled, it will not run at the scheduled time.
 **NOTE:** If the schedule was enabled on some systems and disabled on others, selecting *Enable* will enable it on all systems. Likewise, selecting *Disable* will disable it on all systems.
 - **In Use** displays *Yes* if any entities are assigned to this schedule.
4. Select **Close** when you are finished.

Adding or editing physical capacity measurement schedules

You can add or edit physical capacity measurement schedules using the Manage Measurement Schedules dialog.

About this task

 **NOTE:** If you change the name of a Tenant that is part of a PCM schedule, the name change is not updated automatically in the schedule. You must manually add the new Tenant name to the PCM schedule.

Steps

1. Select **Capacity > Management > MTree tab > Physical Capacity Measurement > Schedules**
2. In the Manage Measurement Schedules dialog, select Add (green plus sign), or select a schedule and select Edit (yellow pencil).
3. In the Add a Schedule or Edit *schedule* dialog, enter or edit the following information:
 - **Status** is displayed only for editing. Select *Enabled* or *Disabled*.
 - **Name** can be entered only for a new schedule. You cannot edit the name after the schedule has been created.
 - **Every** can be *Day*, *Week*, or *Month*. Selecting *Week* or *Month* will bring up a weekly or monthly calendar where you can select the days of the week or days of the month.
 - **Scope** indicates whether the schedule is *MTree*, *Tenant*, or *Tenant Unit*. You cannot create a schedule with different types of entities; however, you must select one to create a schedule. You cannot edit the scope after it has been created.
 - **Assignment** displays *Yes* if any entities are assigned to this schedule.
4. Select **Add**.

Deleting physical capacity measurement schedules

You can delete physical capacity measurement schedules using the Manage Measurement Schedules dialog.

Steps

1. Select **Capacity > Management > MTree tab > Physical Capacity Measurement > Schedules**
2. In the Manage Measurement Schedules dialog, select a schedule, and select Delete (red X).
3. In the Delete *schedule* dialog, select the down arrows beside **More information** to see the entities assigned to this schedule.

4. Select **Yes** or **No**.

Assigning and unassigning measurement schedules for physical capacity

You can assign and unassign measurement schedules for physical capacity of MTrees, Tenant Units, or Tenants, using the Assign/Unassign Schedules dialog. Assigning a schedule to a Tenant will measure that Tenant on all DD systems used by the Tenant.

Steps

1. Select all or multiple MTrees, a single MTree, a Tenant Unit, or a Tenant for which you want to assign or unassign schedules.
2. Select **Capacity > Management > MTree tab > Physical Capacity Measurement menu > Assign/Unassign Schedules**.
3. In the Assign/Unassign Schedules to *entity* dialog, you can move schedules from the Available Schedules list to the Assigned Schedules list, and vice versa, using the arrows. The double arrows (>> and <<) move everything. The single arrows (> and <) move only the selected schedule.
4. Select **Save** or **Cancel**.

Measure now for physical capacity

You can perform a *measure now* task, that is, a one-time measurement, for physical capacity of MTrees, Tenant Units, or Tenants, using the Measure Now dialog box.

Steps

1. Select all or multiple MTrees, a single MTree, a Tenant Unit, or a Tenant that you want to *measure now*.
2. Select **Capacity > Management > MTree tab > Physical Capacity Measurement menu > Measure Now**.
3. In the Measure Now dialog box, you can select **Hide** to keep the process going, but to not show the dialog box. You can monitor progress on the Jobs page.
 - a. If the job submits successfully, a success message is displayed.
 - b. If the job fails, the reason for failure is displayed when hovering over the "Failed" status.
 - c. For entities associated with multiple systems (a single Tenant or multiple MTrees), if an error occurs, a table with the error on a per Data Domain system basis is displayed.
 - d. After the job starts, it may take some time for it to complete.

 **NOTE:** A physical capacity measurement takes roughly the same time as a cleaning cycle. This might be hours or, in extreme cases, days. Timing depends on the current workload of the system and how much data is in the MTree, Tenant Unit, or Tenant.

It may take up to an hour for the physical capacity measurement data to show up on the MTree pages after the job is completed.

Viewing physical capacity measurement jobs

Use the **View Measurement Jobs** dialog to view physical capacity measurement jobs, for either an MTree, a Tenant, or a Tenant Unit.

About this task

The number of physical capacity measurement samples that are presented by the DDMC is typically different from the number of samples that are shown by the DD OS. The DD OS prunes historical physical capacity measurement samples for MTrees, Tenant Units, and Tenants daily and keeps the distribution of historical samples for no more than one sample per hour for the last 90 days, and then no more than 1 per day for the last year, then no more than 1 per week for the last 10 years. DDMC prunes physical capacity measurement samples and keeps at most 730 days of PCR data. Because it does not have regular periodic data, it is pruned like alerts.

Steps

1. Select **Capacity > Management > MTree tab > Physical Capacity Measurement > View Measurement Jobs**

2. In the View Measurement Jobs for *entity* dialog, observe the combined list of physical capacity measurement jobs that are In-progress, Completed, and Failed, starting with the most recent.
3. Select **Close**.

Checking projected system capacity

The **Capacity > Projected** page helps you plan future capacity needs.

You can use this information to:

- Predict when systems will run out of storage space or reach a critically low point
- Determine future capacity needs by projecting historical and current trends
- Determine targets for migration by projecting the systems that are filling up, versus the same model systems that will have space available
- Perform CSV export

Each entry in the table shows the system name and a connection status icon with a pop-up containing a link to the **Health > Alerts** page. The space usage amounts (size, used, and free) for current and projected months are provided. A storage graphic depicts the system's capacity by percentage that is used, with color coding to show normal, warning, and critical threshold levels. This graphic is a thumbnail version of the default projection chart at the bottom of the page.

The Projected Capacity (By Date) control presents information in three groups of columns. There is also a *sparkline* chart to present the general shape of the variation.

- 100% Capacity shows the projection when the system will be 100% full, based on the automatically determined growth rate.
- Projected Capacity lets you compute the used capacity on a specific date. The system might have free capacity, be full, or be overfull. These columns project just how much over capacity the system will be, so you know how much capacity you need to free up or buy.
- Current Capacity simply shows the current state of the Data Domain system, which is the same as the **Capacity > Utilization** page.

If insufficient data prevents an accurate projection, informational messages are displayed.

Table 9. Insufficient data messages

Message	Description
Data is no longer being added to system.	The used capacity is flat, so predictions are unreliable.
Projection cannot be made.	The projection failed for unknown reasons.
Projection cannot be made because the average space used in the last 7 days is less than 10%.	The system has so little data that the file system is less than 10% used. A projection cannot be made when such a small amount of capacity is used because it is unreliable.
Projection cannot be made because of insufficient data. A minimum of 15 daily space usage points is required for projections.	At least 15 days of data is required to make a reliable projection.
<ul style="list-style-type: none"> • Projection cannot be made because of a large recent drop in space used. • Projection cannot be made because the usage trend is not consistent during the past 15 days. 	A regression was computed, and the slope is negative (that is, capacity is freeing up, not being consumed), and the fullness date is in the past.
Projection cannot be made because the space used varies too greatly during the past 15 days.	The last measured usage point is below the confidence interval of the projection. The confidence interval is the 95% band, that is, for 95% of the time, the actual data points should be within the confidence interval. The most recently measured point is lower than the lowest value expected with 95% confidence.
Projection cannot be made because a specific pattern based on the most recent space usage data cannot be determined.	A regression was computed, but the best regression does not match the actual measurements closely. Technically, this result indicates that the R ² value (the "coefficient of determination") is less than 0.8. [An R ² value of 1 means a perfect fit was found. A value of 0 means that no correlation was found at all.] This R ² value means that capacity is not being used in a smooth, linear fashion. It is either being consumed at a varying rate or

Table 9. Insufficient data messages (continued)

Message	Description
	varying between being used and freed up. (See Space projection algorithm for DDMC on page 43 for more about R ² .)

Date column data (Current, and those selected using the timeline) can be sorted by amount of Used Space, Free Space, % Used, and Size in rising or descending order.

Highlighting a system in the list activates controls for interactively customizing the projection and launching the DD System Manager.

Interacting with the Projection Chart

You can perform a custom projection using the interactive Projection Chart at the bottom of the **Capacity > Projected** page.

Steps

- To adjust the visible range of data shown in the chart (this does not change the projected dates):
 - In the Date Range control, at the top left of the chart, simply select 1w, 1m, 3m, 1y, or All. The input fields at upper left change the visible range of data, and those on the right change the projection dates.
 - Enter specific dates in the date input fields.
 - To change the projections, you can slide or adjust the gray area in the chart. You can move these controls to the left or right, or you can make the chart wider or narrower, to fit a time range you believe is more representative than the one DDMC computed as the best fit.

A better correlation between the projected trend line will show a narrower confidence range around the projected trend line. A less satisfactory correlation will show a wider confidence range.

- In the Dates used for making projections control, at the top right of the chart, the dates will update to reflect the customized projection.
- Use the Defaults button to return to the default/best fit projections.

Checking the System Details lightbox

The *System Details lightbox* provides detailed operating information about specific components of a Data Domain or PowerProtect system.

There is a **System Details** control on each of the following pages:

- **Health > Status**
- **Capacity > Utilization**
- **Capacity > Projected**
- **Replication > Overview**
- **Inventory > Systems**

To activate the control, you must first select a Data Domain system from the table.

There are five tabs for non-HA systems, and six tabs for HA systems.

The **Overview** tab shows the operational status of various system components (such as the file system and protocols) using LED status indicators. Also provided are summaries of file system usage and capacity, and replication status and statistics for inbound and outbound replications.

The **Capacity** tab shows different tier data if applicable. If the configuration is a single-tier system, there is only one column. If the configuration is a Cloud or Extended Retention tier system, then there are Active tier, Cloud or Retention tier respectively, and total columns. This tab contains a Capacity usage chart and a table with MTrees on that system.

The **Network** tab shows total bytes, backup and restore bytes, and replication inbound and outbound bytes. There is a network byte chart as well.

The **Charts** tab lets you produce charts for selected time intervals. System Charts tab has all of the system charts. For cloud enabled systems, charts are broken into two sections - Historical, which contain the same charts as before, and a new Current charts section, which contains two pie charts that show the current distribution of data on the systems and cloud providers. These charts are:

- Protection Distribution - a chart showing how much data resides on-premises versus on different cloud providers.
- Licensed Capacity Usage - Space that is used on each provider, space available, and total capacity licensed for all the providers combined.

The **Replication** tab lists the counts of different automatic/on-demand replication pairs, both inbound and outbound, with ones that have errors or warnings. There are also inbound and outbound charts.

The **HA** tab, for an HA system, contains the HA system health diagram which marks alerts, if any, in each component of the HA system. Selecting different components in the diagram can filter the alerts that are viewed in the table.

Resource charts

- **CPU utilization** shows the CPU utilization percentage for the system by date and also shows when cleaning is being performed.
- **Network throughput** shows whether a system is experiencing bandwidth-related bottlenecks. You can determine how much network bandwidth is being used by systems sharing the same subnet to see if any are using more than expected or enabled by IT departments.

File system charts

- **Streams counts** shows the numbers of each type of stream that were open at the date and time that is indicated for each data point. It is not an aggregate (average, min, or max) of the stream count over the selected interval. It is best viewed at the lowest interval (hourly), so that hourly stream count throughout each day can be observed. At greater intervals (daily or weekly), only a single data point, which is taken at noon, is shown, which is not helpful in determining how many streams were open throughout the day or week. In summary, the hourly interval is the best choice for viewing this chart.
- **Protocol processing** shows the number of operations per second.
- **Protocol throughput** shows the following:
 - **Data in** is the amount of data that the DD OS file system can read from the kernel socket buffer.
 - **Data out** is the amount of data that the DD OS file system can write to the kernel socket buffer.
 - **Wait Time per MiB in** is the amount of time it takes for the DD OS file system to receive one mebibyte of data from a network client. A high value indicates that the client is sending data relatively slowly and any performance issues are likely to be related to the client or network. A low value indicates that data is arriving from a network client as fast or faster than it can be deduplicated and written to disk.
 - **Wait Time per MiB out** is the reverse metric, the amount of time that is taken to send a mebibyte of data from the DD OS file system to a network client. A low value indicates that data can be sent over the network as fast as it is being read from disk. A high value indicates that data is being read from disk faster than it can be accepted by the network and network client.

Replication charts

- **Inbound characteristics** shows the inbound counts for both automatic and on-demand replication pairs.
- **Outbound characteristics** shows the outbound counts for both automatic and on-demand replication pairs.
- **Throughput** shows throughput for both automatic and on-demand replication pairs.

Monitoring replication

The Replication pages provide status and performance details about replication pairs – organized by Data Domain or PowerProtect systems, Groups, or Tenants. For each page, you can view either pairs, cascades, or topology by selecting the controls at the upper right.

 **NOTE:** For Automatic and On-demand pages, Group view has different behavior than Tenant view. Groups view shows ungrouped pairs while Tenant view do not show pairs that do not belong to any tenants or tenant units.

For Tenants – in the **Replication > Overview > All Pairs** page:

- Grouping hierarchy is Tenant, Tenant Unit, Inbound, Outbound, Automatic, On-demand, Replication pair. If there are no applicable replication pairs, the corresponding row will not appear.
- If a Tenant Unit has no MTrees or Storage Units participating as a Source or Destination, that Tenant Unit is not displayed.
- MTrees and Storage Units that are not assigned to any Tenant Units are not displayed, even if they may be a source or destination. Similarly, if all Tenant Units in a Tenant have no MTrees or Storage Units with Replication contexts, that Tenant is not displayed.
- RBAC (role-based access control) also affects the Tenants and Tenant Units that are displayed.
- The CSV (comma-separated values) file contains these additional columns: Tenant, Tenant Unit, Source Tenant, Source Tenant Unit, Destination Tenant, Destination Tenant Unit. It does not contain the System column.
- Replication pairs are grouped by the Tenant or Tenant Unit to which the source or destination MTrees or Storage Units belong.

- A pair will be listed twice when the source and destination belong to different Tenant Units.

For Tenants – in the **Replication > Overview > Topology** page:

- The source or destination shows the Tenant Unit name if the MTree or Storage Unit belongs to a Tenant Unit.
- Tenant Units are shown inside systems. The Tenant name is shown above the Tenant Unit icon.
- Tenant Units can be expanded just like systems.
- MTrees that do not belong to a Tenant Unit are displayed if one end of the pair belongs to a Tenant Unit.
- Tenant Units not assigned to a Tenant are displayed if one of their MTrees or Storage Units has a replication to or from an MTree or Storage Unit belonging to a Tenant Unit.
- Cascaded replications are still displayed if they include data that originates from or is replicated to a managed Tenant Unit.
- The context menu for a Tenant Unit includes menu items for Tenant and Tenant Unit detail lightboxes.
- You can choose the *related pairs view* for a Tenant Unit or Tenant.
- The related pairs view for a Tenant shows all Tenant Units from that Tenant, and incoming, outgoing, or cascaded pairs from its Tenant Units.

For Tenants and Systems – in the **Replication > Overview > All Pairs** page:

- Each monitored DD system or Tenant that has configured replication pairs is listed.
- Expand an entry to see its inbound and outbound replications, and for these, expand to see the replication type: Automatic (Data Domain or PowerProtect system to Data Domain or PowerProtect system replications) and On-demand (client-initiated and controlled replication of DD Boost files), and expand those to see the pairs of that type. The Inbound and Outbound entries are shown only when applicable.
- Use the column selector to display columns for replication status, number of pairs (totals for systems, inbound, and outbound replications), and a selectable/configurable time-interval for displaying historical replication data.
- Double-click a status error icon at the system level to open the System Details Lightbox, where hovering on the Replication LED exposes a pop-up with a link to the Alerts page, which is filtered for the pairs in error. The Status error icon for a category (inbound, outbound, system) shows if any of its items has an error condition.
- Use the right triangle **System** control at the upper left of the table to expand the inbound and outbound tiers to see all Automatic and On-Demand replications (if the system entries have not been expanded yet), and also to collapse all expanded entries.

For Systems, Groups, or Tenants – in the **Replication > Automatic** page:

- All monitored system replications for directory, collection, and MTree replication are listed.
- The page banner displays the total count of monitored Automatic replications, and the table shows for each replication pair selectable columns for the status, source and destination systems, and performance data, such as lag time (the lag cell is red when lag duration is greater than or equal to the Critical threshold and yellow for Warnings; hover over the cell for detailed information about the lag threshold), lag trend (increasing – the data cannot be replicated within the lag threshold), steady, decreasing, or no arrow if the pair is suspended or in error), time over threshold (hover to see policy settings), bytes remaining, and status message text.
- The page-specific controls include **Assign Properties** and **Lag Threshold Policy/Manage Lag Threshold Policies** to set/manage alerting for when an Automatic Replication lag time exceeds the set time limit for critical and warning levels.

For Systems, Groups, or Tenants – in the **Replication > On-Demand** page:

- Historical data for completed replications can be viewed for the past 24 hours, 7 days, 30 days, 90 days, or by setting a custom time frame.
- Details that are shown are for Pre-comp data that is replicated, completed and failed replicated files, percentage of failure, and the last error messages.
- For the group view, data for pairs are rolled up at each group level. Data for all pairs are summarized at the last line of the table.
- The number of completed and failed files can include file replications that the system retried up to four times due to recoverable failures. The sum of the completed and failed file replications can be greater than the total number of file replications that were initiated by the DD Boost applications on the replication pair.
- DD Boost file replications are listed (for systems running DD OS 5.3.1 or later), showing for the pair: the last transfer status, source and destination storage units, and performance data for recent and completed replications. The table can be organized by Pairs or Groups (switch at upper right).
- If the source or destination fields show an IP address instead of a hostname, the DNS server configuration for the Data Domain system must be modified. When configuring Data Domain systems to monitor DD Boost (on-demand replication), ensure that their DNS servers include configuration for both forward and reverse hostname lookup. Without proper DNS server configuration, Data Domain systems cannot translate from IP addresses to host names, and the source and destination paths contain IP addresses instead of host names.
- The replication **Pair Details** control is active when a pair is selected and shows a lot of replication detail.
- The **System Details** control is active when a system entry is selected on the **Overview** page.

- The **Export CSV file** control sends the overview listing with performance data for the last 7 days to a file with comma-separated values (for viewing in Excel, for example).

Viewing replication topology to investigate error conditions

When the **Topology** view is selected on the **Replication > Overview** page, it shows the relationships of the site's configured replication contexts and uses color-coded status indicators and other map controls to let you easily locate and drill-down to investigate error conditions.

Use the **Type** menu to select the replication types that are shown in the map work area (MTree, directory, collection, and on-demand files). If a replication type has not been configured among the site's replications, its checkbox in the menu is disabled. If a type is enabled but de-selected, those node relationships do not show on the map.

A slider on the map controls the scope of replication contexts that are shown in the work area display.

The inset is a miniature representation of the map and its scope is controlled by the slider manipulation. The inset itself can be selected and moved around to include or exclude systems in the map work area.

Replications statuses between systems are shown with color-coded directional lines, which will show red if any of the replications is in error. Hovering over the line shows the number of replication pairs and a count for each status level.

The action buttons above the graph correspond to the selected item in the graph. Selected items can be:

- System (Buttons for system details and launching DD System Manager will show.)
- Tenant Unit (Buttons for tenant or tenant unit details will show.)
- Property or Data Set (MTree, directory, collection, etc.)

Use the actions items to show **Related Items** and **Connected Items** available for any object selected in the graph to show an in-depth view of all replication pairs that are configured. Items related to a selection will include all pairs with direct replications or cascades connected to the selected items. The **Connected Items** button will filter to show a connected graph containing the selected item. (A graph is connected if there is a path between every pair of graph nodes.)

The right panel lists the **Replicated Pairs** (of highlighted systems in the map work area or all contexts if nothing is highlighted), showing the type of context, source and destination systems, status, with a link to additional details. Selecting a context activates the **Pair Details** control.

Checking the Replication Pair Details lightbox

Selecting a replication pair on any of the Replication pages activates the **Pair Details** control, which opens the *Replication Pair Details lightbox*.

There are two tabs: Overview and Charts.

The **Overview** tab shows:

- The last transfer status
- The source and destination systems
- Settings such as encryption and operational status
- Color-coded icons showing capacity levels

The **Charts** tab provides graphs for:

- Pair characteristics - performance factors, such as pre-compression written, pre-compression replicated, post-compression replication, pre-compression remaining, network bytes, and compression ratio.
- Lag trend - charts pre-compression remaining, replication lag, pre-compression written, warning threshold, and critical threshold (not available for on-demand replication)
- CPU utilization
- Data written
- Network and replication throughput
- Source and destination characteristics, as well as common pairs

The charts are vertically aligned for source and destination systems by the same time interval, allowing comparisons for both systems at any point in time.

Possible reasons for "SU is unresolved" message

If a Storage Unit for a DD Boost replication pair shows the message, "SU is unresolved", here are some possible reasons:

- The remote system is not registered with DDMC.
- Both systems are registered, but one is running an unsupported DD OS version and is not able to report the Storage Unit name.
- The remote hostname is an IP address and cannot be matched to a registered hostname.

Monitoring status with reports

Reports compile information for areas of interest on managed systems and for Secure Multi-Tenancy (SMT) and DD Cloud Tier.

Reports are generated based on default report template types. Report templates configure the report's content, schedule, and email distribution.

NOTE: If a user who is the "owner" of any report templates is deleted from the CLI, those report templates will still appear to be owned by the "deleted" user, but the reports will no longer run at their scheduled times.

There are three default report template types for systems:

- Capacity (Capacity Overview)
- Replication (Replication Status)
- Status (Current Health Status)

There are two default report template types for SMT and Cloud Tier:

- Status (Daily Status)
- Usage (Usage Metrics)

Creating a report with the wizard

The Add Report Template wizard creates a report template for use in running reports about key data points.

About this task

NOTE: The number of physical capacity measurement samples that are presented by the DDMC is typically different from the number of samples that are shown by the DD OS. DDMC displays more samples because it does not do any pruning on physical capacity measurement samples. The DD OS prunes historical physical capacity measurement samples for MTrees, Tenant Units, and Tenants daily and keeps the distribution of historical samples for no more than one sample per hour for the last 90 days, then no more than 1 per day for the last year, then no more than 1 per week for the last 10 years.

Steps

1. Select **Reports > Management**.
2. Select Add (green plus sign).
3. In the Add Report Template dialog, select the type of report you want (System Reports, Multi-Tenancy Reports, or Cloud Reports), and select **Next**.
4. Enter a name, and select a Template. Choose one or more Sections to include, and select **Next**.
 - a. For System, the choices are Capacity, Replication, or Status.

The **Hide capacity projection data** checkbox will appear after a **Template** is selected from the dropdown. Selecting this checkbox hides the projection data from the report.
 - b. For Multi-Tenancy, the choices are Status or Usage.
 - c. For Cloud Tier, the choices are Status or Usage.
5. Depending on whether you selected System, Multi-Tenancy or Cloud Tier:
 - a. System: Select a filter to narrow the scope of reported objects (for example, filter by selected groups). Select the time span for data collection (for example, last 24 hours), and the report retention (for example, 7 days). Select **Edit** to set a schedule for the frequency and time the report is run. Report generation time will be two hours ahead of *Starts On* time. Select **Next**.

- b. Multi-Tenancy: Select a Scope (**Tenant Unit** or **Tenant**). The Daily Status report is always configured to show the last 24 hours of historical data, and you can select the Report retention (Forever, 7 days, 30 days, 90 days). The Usage Metrics report (which is generated as an Excel spreadsheet) lets you display data for a full month or a full week. Select **Edit** to set a schedule for the frequency and time the report is run. Report generation time will be two hours ahead of *Starts On* time.
 - c. Cloud Tier Reports: Select **Cloud Service Providers** to filter the systems that have cloud tier that is configured to connect to them.
6. Optionally, add recipient email addresses (for when the report completes and if an error occurs). For the Tenant Unit report template, the Tenant Unit admin email messages are added by default. For the Tenant report template, the Tenant admin email is added by default. You can manually add or remove these email messages. Select **Next**.
 7. Review the details, and select whether to save the template for later use and to run the report immediately. Select **Finish**.

Results

After it has been created, a report template is added as an entry in the reports table. When selected, the report template can be used to immediately run a report, or it can be edited or deleted, or the time it was last run can be displayed.

Edit report

Properties of an existing report template can be edited.

Steps

1. Select **Reports > Management**.
2. Select the template name, and click Edit.
3. In the Edit Report Template dialog, choose the report property to edit.
 - Content - Template name, template that is used, and sections.
 - Scope - Systems in the report.
 - Schedule - Status, time span, schedule run time, and report retention
 - Email - Add and delete email addresses where reports are sent when the report is finished and if an error occurs. Capacity reports have the option to have the content embedded within the email. The report is sent as an email attachment by default.

Generating a report immediately

To generate a report immediately, select a report template that is listed in the Template name table, and select **Run Report**.

A report (named by concatenating the data stamp to the template title) is created and opened as a .PDF file in your browser, except for the Tenant Usage and Cloud Usage reports, which generate an .xlsx file.

The report generation information is listed in the Report History table, where it can be viewed, renamed, or deleted.

Cleaning up reports from deleted users

Report templates owned by deleted users can be deleted, or re-assigned to another DDMC user.

Users can be deleted from the **Settings > Access > Local Users** window.

When deleting a local user, DDMC provides the option to select another local user to own the deleted user's report templates, or delete the report templates along with their owner. Report templates are re-assigned to sysadmin by default, but any local user can be selected.

If the report templates are re-assigned, the report schedules are disabled by default until the email recipients for the report are updated. Report templates can be updated from the **Report Management** window, or the **Edit** button on the **Schedule** tab.

Managing Data Domain and PowerProtect Systems

Topics:

- [Launching DD System Manager](#)
- [Upgrading system software](#)
- [Local users](#)

Launching DD System Manager

From some DDMC pages, you can launch a DD System Manager session to perform configuration or troubleshooting. The launched version of DD System Manager runs on DDMC, not on the system, which gives a centralized, secure, and simultaneous administration for multiple systems.

To start a session, select an entry in a table listing (for example), and select **Launch DD System Manager** from any of the following DDMC pages:

- **Health > Status**
- **Capacity > Management**
- **Capacity > Projected**
- **Inventory > Systems**
- **Replication Pair Details** lightbox
- **System Details** lightbox

The DD System Manager session that starts requires no login or logout and provides complete management of the system. DD System Manager opens showing the corresponding area from where it was launched (for example, if the launch was from the Alerts view, the Alerts page on the Data Domain system is opened).

 **NOTE:** In **Classic view**, DD System Manager opens in a new window. Ensure that the pop-up blocker on your browser is configured to enable pop-ups for DDMC.

The launched DD System Manager is displayed inside DDMC, and the navigation menu is changed to the DD System Manager menu. A **Back** button is on the upper left with the system name shown underneath. Clicking the **Back** button navigates back to the DDMC module that launched the DD System Manager.

Note the following about launching DD System Manager from DDMC:

- You can launch DD System Manager for a system for which you have an *admin*, *limited-admin*, or *user* role.
- A permission is composed of a system or group, a user (local or NIS), and a role.
 - The administrator role is required for replication configuration and IPMI configuration.
- The inventory of systems on DDMC is used.
 - The systems that are shown are based on the effective permissions.
 - Only replication source and destination systems that are registered with DDMC are shown.
- Other firewall ports for the session do not need to be opened. After a system is added to DDMC, the existing port assignments are used for the DD System Manager connection.

Upgrading system software

You can upgrade the DD OS on one – or a group of – Data Domain and PowerProtect systems, if you have admin rights on those systems and on DDMC.

Procedure

NOTE: HA systems cannot be upgraded from DDMC. Launch DD System Manager for the HA system and perform the upgrade on the system itself.

1. Get a DD OS upgrade package, by downloading an upgrade package from the online support site at <https://support.emc.com/>.
2. Upload the DD OS upgrade package to the DDMC inventory.
3. Perform the DD OS upgrade on the systems.

Managing system upgrade packages

Before you can upgrade a Data Domain or PowerProtect system through DDMC, you must upload the upgrade package to the DDMC. The DDMC admin can manage packages (add and delete) on the **PACKAGES** tab.

Steps

1. Select **Inventory > Upgrades**.
Two tabs are now available in the main window: **SYSTEMS** and **PACKAGES**.

2. Select **PACKAGES**.

3. Click on add button to add the software package
After the upgrade package has been uploaded to the DDMC, you can upgrade one or more systems.

NOTE: To delete a package, check the box next to a Package Name and click **DELETE** to remove that software package.

Performing a system upgrade

The DD OS on one or more Data Domain and PowerProtect systems can be upgraded from DDMC with one upgrade operation. If systems are not in an acceptable managed state (for example, unreachable, suspended, upgrading) the upgrade action is unavailable.

About this task

NOTE: For security reasons, there is a 30-minute time limit for the upload of RPM packages for DDMC and DD system upgrades using the DDMC GUI. If you have a slow connection from a client machine to the DDMC and the upload takes more than 30 minutes, the connection drops and you cannot use DDMC to upload the package.

Workaround: Use the CLI to upload the package into DDMC (for example, use `SCP/PSCP` from a Unix terminal or Windows CMD).

For DDMC upgrades, upload the package to `/ddr/var/releases`.

For DD System upgrades, upload the package to `/ddr/var/ddr-releases`.

Steps

1. Select **Inventory > Upgrades**.
Two tabs are now available in the main window: **SYSTEMS** and **PACKAGES**. **SYSTEMS** is selected automatically and a list of ungradable systems are displayed.
2. Select one or more systems to upgrade.
If there was a precheck error, there is an option to run precheck manually from details panel after fixing any errors.
3. Click the **ON-DEMAND** dropdown and select one of the three options:
 - **Distribute** - push an RPM to the selected system or systems.
Select the wanted DD OS version from the drop-down list in the **On-Demand Distribute** dialog . Click **Distribute**.
 - **Upgrade** - upgrade the selected system or systems.
Select the wanted DD OS version from the drop-down list in the **On-Demand Upgrade** dialog. Click **Upgrade**.
 - **Distribute and Upgrade** - push RPM and then upgrade the select system or systems.

Select the wanted DD OS version from the drop-down list in the **On-Demand Distribute and Upgrade** dialog. Click **Upgrade**.

 **NOTE:** HA systems cannot be upgraded from DDMC. If one or more HA systems are selected, DDMC displays a message stating that upgrades for HA systems are not supported.

Once the operation is started, the admin can click the icon in the **Details** column where a detail panel will slide in to show detail activities happening on the selected system. The detail panel can be shown only one system at a time.

Local users

Local users are non-administrative users that can log into DDMC, but can only view systems specified by an administrator.

Creating access for users

To set up access to DDMC, you must add users and access groups and add permissions for certain roles.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Local Users**.
2. Click **Add** to create users.

These users can log in to DDMC, but cannot see any other systems. You can add permissions to view (user role), administer (admin role or limited-admin), or take snapshots (backup operator) for groups and systems.

User groups have either admin or user roles; user roles can be admin, limited-admin, and user. If a user or a user group has the admin role, they can view all Data Domain systems by default; it is not necessary to set any other permissions for admin users and groups.

3. **Access Authentication** to create access groups (NIS and Active Directory) in DDMC.
4. For users and user groups with the user role, you must set permissions on systems so they can view the systems. Select **Administration > Permissions**.
5. Select Add (green plus sign).
6. In the Add Permissions dialog, select where to add the permission:
 - **Add permissions to systems** – Select this option, and from the list of managed systems, select the checkboxes of the systems where the permissions are to be assigned.
 - **Add permissions to groups** – Select this option, and from the list of groups, select the checkboxes of the groups where the permissions are to be assigned.
7. In the User area, select Add (green plus sign), select one or more users from the Select Users dialog, and select **Select**.
8. Click in the Role field for the user, and select the access role: Administrator, Limited-Admin, Backup Operator, or User.
9. Select Add (green plus sign).

The users are given the assigned role (Administrator, Limited-Admin, Backup Operator, or User) for the selected systems or groups.

Next steps

To simplify the management of permissions:

- It is recommended that the use of the admin role for the DDMC be minimal.
 - The admin role can manage all Data Domain systems in the DDMC inventory. In addition, the admin for the DDMC configures the DDMC properties and groups and assigns its permissions.
 - Configure most logins for DDMC with the user role.
- Use NIS user groups for permissions – this simplifies the process for adding, removing, and modifying users without changing the permission assignment.
- Use DD System Groups for permissions rather than assigning permissions to individual systems.

By assigning permissions at the group level, policy-based permissions can be used with a union model that is applied to the entire group hierarchy.

- Start with lower-level permissions at the top of the hierarchy:
 - Assign lower-level permissions toward the root of the Group hierarchy.
 - Assign higher-level permissions toward the leaf of the Group hierarchy.
 - Use a union model, not an override model. This makes it easy to change permissions at lower levels without affecting the entire hierarchy.

Verify Changes:

- After assigning permissions or changing group membership, verify the change by looking at the Effective role for a system.

Use Central Administration:

- Use DDMC to centrally administer all systems, reducing the use of local accounts on each managed system. Turn off direct GUI access to systems that are managed by DDMC.

Understanding DDMC permissions

The **Administration > Permissions** pages (Assigned, Groups, Systems, Users) show the permissions of DDMC users by assigned role.

Permissions are a "triangle" of three components:

- the managed object (groups or systems)
- the user (local, NIS, or Active Directory)
- the DD System Manager role (Administrator, Limited-Admin, Backup Operator, or User)

The Permissions pages are also used to add, modify, and remove permissions from groups and systems. Each of the views shows the users, their assigned roles, and their effective roles.

Administering Secure Multi-Tenancy

Topics:

- [How DDMC helps with SMT monitoring](#)
- [Creating and managing Tenants](#)
- [Creating and managing Tenant Units](#)
- [Creating, editing, and generating SMT reports](#)

How DDMC helps with SMT monitoring

DDMC can configure and monitor Secure Multi-Tenancy (SMT) for DD Boost backup and replication storage on multiple Data Domain systems.

In a secure multi-tenant environment, storage administrators (*landlords*) and backup administrators (*tenants*) cooperate to allocate and manage storage, as follows:

i **NOTE:** Secure multi-tenancy is not supported on DDVE 2.0 instances, but it is supported on DDVE 3.0 and later.

1. The storage administrator creates Tenants on DDMC.
For example, the storage administrator in a corporate IT organization might create a Tenant for the backup administrator in the finance department.
2. The storage administrator creates one or more Tenant Units on systems to serve as virtual containers for each Tenant.
3. The storage administrator creates one or more MTrees and/or DD Boost Storage Units.
4. The backup administrator configures backup software to use the MTrees in the Tenant Unit as storage targets.

For more information, see the "Secure Multi-Tenancy" chapter of the *DD OS Administration Guide*.

Secure Multi-Tenancy overview

Secure Multi-Tenancy (SMT) is the simultaneous hosting, by an internal IT department or an external provider, of an IT infrastructure for more than one consumer or workload (business unit, department, or Tenant).

SMT provides the ability to securely isolate many users and workloads in a shared infrastructure, so that the activities of one Tenant are not apparent or visible to the other Tenants.

A *Tenant* is a consumer (business unit, department, or customer) who maintains a persistent presence in a hosted environment.

Within an enterprise, a Tenant may consist of one or more business units or departments on a protection system that is configured and managed by IT staff.

- For a business unit (BU) use case, the Finance and Human Resources departments of a corporation could share the same system, but each department would be unaware of the presence of the other.
- For a service provider (SP) use case, the SP could deploy one or more systems to accommodate different Protection Storage services for multiple end-customers.

Both use cases emphasize the segregation of different customer data on the same physical system.

Terminology used in Secure Multi-Tenancy (SMT)

Understanding the terminology that is used in SMT will help you better understand this unique environment.

MTrees

MTrees are logical partitions of the file system and offer the highest degree of management granularity, meaning users can perform operations on a specific MTree without affecting the entire file system. MTrees are assigned to Tenant Units and contain that Tenant Unit's individualized settings for managing and monitoring SMT.

Multi-Tenancy

Multi-Tenancy refers to the hosting of an IT infrastructure by an internal IT department, or an external service provider, for more than one consumer/workload (business unit/department/Tenant) simultaneously. DD SMT enables *Data Protection-as-a-Service*.

RBAC (role-based access control)

RBAC offers multiple roles with different privilege levels, which combine to provide the administrative isolation on a multi-tenant protection system.

Storage Unit

A *Storage Unit* is an MTree configured for the DD Boost protocol. Data isolation is achieved by creating a Storage Unit and assigning it to a DD Boost user. The DD Boost protocol permits access only to Storage Units assigned to DD Boost users connected to the system.

Tenant

A *Tenant* is a consumer (business unit/department/customer) who maintains a persistent presence in a hosted environment.

Tenant Self-Service

Tenant Self-Service is a method of letting a Tenant log in to a protection system to perform some basic services (add, edit, or delete local users, NIS groups, and/or AD groups). This reduces the bottleneck of always having to go through an administrator for these basic tasks. The Tenant can access only their assigned Tenant Units. Tenant Users and Tenant Admins will, of course, have different privileges.

Tenant Unit

A *Tenant Unit* is the partition of a system that serves as the unit of administrative isolation between Tenants. Tenant units that are assigned to a tenant can be on the same or different systems and are secured and logically isolated from each other, which ensures security and isolation of the control path when running multiple Tenants simultaneously on the shared infrastructure. Tenant Units can contain one or more *MTrees*, which hold all configuration elements that are needed in a multi-tenancy setup. Users, management-groups, notification-groups, and other configuration elements are part of a Tenant Unit.

Understanding RBAC in SMT

In Secure Multi-Tenancy (SMT), permission to perform a task depends on the role that is assigned to a user. DDMC uses role-based access control (RBAC) to control these permissions.

All DDMC users can:

- View all tenants
- Create, read, update, or delete tenant units belonging to any tenant if the user is an administrator on the protection system hosting the tenant unit
- Assign and unassign tenant units to and from a tenant if the user is an administrator on the system hosting the tenant unit

- View tenant units belonging to any tenant if the user has any assigned role on the system hosting the tenant unit

To perform more advanced tasks depends on the role of the user, as follows:

admin role

A user with an *admin* role can perform all administrative operations on a protection system. An *admin* can also perform all SMT administrative operations on the system, including setting up SMT, assigning SMT user roles, enabling tenant self-service mode, creating a tenant, and so on. In the context of SMT, the *admin* is typically referred to as the *landlord*. In DD OS, the role is known as the *sysadmin*.

To have permission to edit or delete a tenant, you must be both a DDMC *admin* and a DD OS *sysadmin* on all systems that are associated with the tenant units of that tenant. If the tenant does not have any tenant units, you need only to be a DDMC *admin* to edit or delete that tenant.

limited-admin role

A user with a *limited-admin* role can perform all administrative operations on a system as the *admin*. However, users with the *limited-admin* role cannot delete or destroy MTrees. In DD OS, there is an equivalent *limited-admin* role.

tenant-admin role

A user with a *tenant-admin* role can perform certain tasks only when *tenant self-service* mode is enabled for a specific tenant unit. Responsibilities include scheduling and running a backup application for the tenant and monitoring resources and statistics within the assigned tenant unit. The *tenant-admin* can view audit logs, but RBAC ensures that only audit logs from the tenant units belonging to the *tenant-admin* are accessible. In addition, *tenant-admins* ensure administrative separation when tenant self-service mode is enabled. In the context of SMT, the *tenant-admin* is referred to as the *backup admin*.

tenant-user role

A user with a *tenant-user* role can monitor the performance and usage of SMT components only on tenant unit(s) assigned to them and only when tenant self-service is enabled, but a user with this role cannot view audit logs for their assigned tenant units. Also, *tenant-users* may run the `show` and `list` commands.

none role

A user with a role of *none* is not allowed to perform any operations on a system other than changing their password and accessing data using DD Boost. However, after SMT is enabled, the *admin* can select a user with a *none* role from the system and assign them an SMT-specific role of *tenant-admin* or *tenant-user*. Then, that user can perform operations on SMT management objects.

management groups

BSPs (backup service providers) can use *management groups* defined in a single, external AD (active directory) or NIS (network information service) to simplify managing user roles on tenant units. Each BSP tenant may be a separate, external company and may use a name-service such as AD or NIS.

With SMT management groups, the AD and NIS servers are set up and configured by the *admin* in the same way as SMT local users. The *admin* can ask their AD or NIS administrator to create and populate the group. The *admin* then assigns an SMT role to the entire group. Any user within the group who logs in to the system is logged in with the role that is assigned to the group.

When users leave or join a tenant company, they can be removed or added to the group by the AD or NIS administrator. It is not necessary to modify the RBAC configuration on a system when users who are part of the group are added or removed.

Tenant and Tenant Unit permission table

Permissions for working with Tenants and Tenant Units depend on the role of the user in both DDMC and the system (DD OS).

Table 10. Permission table for tenants and tenant units, DDMC admin and limit-admin

DDMC user/DD OS role	DDMC admin/DD OS sysadmin	DDMC limited-admin/DD OS sysadmin
Tenant		
Create Tenant	yes	yes
Edit/delete Tenant with no Tenant Units	yes	yes
Delete/destroy MTree	yes	no
Edit/delete Tenant with Tenant Units ^a	yes	yes
View all Tenants defined in DDMC	yes	yes
Display issue with Tenant Units for Tenant in summary page	yes	yes
View Tenant Details lightbox	yes	yes
View MTree configuration issues for Tenant in summary page	yes	yes
Tenant Unit		
See system for selection in the Create Tenant Unit Wizard	yes	yes
Edit and delete Tenant Unit	yes	yes
View Tenant Units that are associated with systems listed in inventory page	yes	yes
Edit/delete unmanaged Tenant Unit	yes	yes
Assign/unassign Tenant Unit to/from Tenant	yes	yes
View Tenant Unit Details lightbox	yes	yes

a. DDMC admin or limited-admin must have DD OS sysadmin or limited-admin role on all Data Domain systems that host the Tenant's Tenant Units.

Table 11. Permission table for Tenants and Tenant Units, DDMC user

DDMC user/DD OS role	DDMC user/DD OS sysadmin or limited-admin	DDMC user/DD OS user or backup operator	DDMC user/no DD OS role
Tenant			
Create Tenant	no	no	no
Edit/delete Tenant with no Tenant Units	no	no	no
Delete/destroy MTree	no	no	no
Edit/delete Tenant with Tenant Units	no	no	no
View all Tenants defined in DDMC	yes	yes	yes
Display issue with Tenant Units for Tenant in summary page ^a	yes	yes	no
View Tenant Details lightbox ^b	yes	yes	no
View MTree configuration issues for Tenant in summary page ^c	yes	yes	no
Tenant Unit			

Table 11. Permission table for Tenants and Tenant Units, DDMC user (continued)

DDMC user/DD OS role	DDMC user/DD OS sysadmin or limited-admin	DDMC user/DD OS user or backup operator	DDMC user/no DD OS role
See system for selection in the Create Tenant Unit Wizard	yes	no	no
Edit and delete Tenant Unit	yes	no	no
View Tenant Units associated with systems listed in inventory page	yes	yes	no
Edit/delete unmanaged Tenant Unit	yes	no	no
Assign/unassign Tenant Unit to/from Tenant	yes	no	no
View Tenant Unit Details lightbox	yes	yes	no

- a. For DDMC users, only aggregate/show the Tenant's Tenant Units on system for which the DDMC user has a DD OS role (sysadmin, limited-admin, user or backup operator)
- b. For DDMC users, only aggregate/show the Tenant's Tenant Units on system for which the DDMC user has a DD OS role (sysadmin, limited-admin, user or backup operator)
- c. For DDMC users, only aggregate/show the Tenant's Tenant Units on system for which the DDMC user has a DD OS role (sysadmin, limited-admin, user or backup operator)

Use cases for SMT

The following use cases summarize how SMT (Secure Multi-Tenancy) can be deployed in protection storage infrastructures.

Local backup

In a local backup use case, a protection storage infrastructure is shared across clients, and deployment is local to the enterprise. The on-premises IT staff uses each Tenant Unit to back up the data of a specific business unit.

Replicated backup

In a replicated backup use case, the tenant performs local backups at their physical site, but does not want to own or manage a remote site for disaster recovery purposes. For this type of tenant, service providers can host multiple tenants, each replicating to their own Tenant Unit, to provide replicated backup services on a shared Data Domain backup appliance platform.

Remote backup

In a remote backup use case, a client does not perform local backups at the physical site. Instead, the client performs direct backups over the WAN to a hosted backup IT environment managed by a service provider or a hosted provider. Remote backup is used for traditional client-based backup and application-direct backup.

Multi-User DD Boost and Storage Units in SMT

When using Multi-User DD Boost with Secure Multi-Tenancy (SMT), user permissions are set by Storage Unit ownership.

Multi-User DD Boost refers to the use of multiple DD Boost user credentials for DD Boost Access Control, in which each user has a separate username and password.

A *Storage Unit* is an MTree configured for the DD Boost protocol. A user can be associated with, or "own," one or more Storage Units. Storage Units that are owned by one user cannot be owned by another user. Only the user owning the Storage Unit can access the Storage Unit for any type of data access, such as backup/restore. The number of DD Boost user names cannot exceed the maximum number of MTrees. (See the "MTrees" chapter in this book for the current maximum number of MTrees for each model.) Storage Units that are associated with SMT must have the *none* role that is assigned to them.

Each backup application must authenticate using its DD Boost username and password. After authentication, DD Boost verifies the authenticated credentials to confirm ownership of the Storage Unit. The backup application is granted access to the

Storage Unit only if the user credentials that are presented by the backup application match the user names associated with the Storage Unit. If user credentials and user names do not match, the job fails with a permission error.

Managing Tenant users and their privileges

There is no direct way to create a Tenant user. The only way for a Tenant to have users is by association with its Tenant Units. Tenant users are all users in their own Tenant Units.

Adding a user with an association to DD Boost data access or Tenant self-service using the CLI can be dangerous because of cross-tenancy issues. The CLI will not validate users belonging to other Tenants when adding DD Boost data access users or Tenant self-service users to the current Tenant.

You can create local users with DDMC. If you create a local user with a role of *none* using the DD System Manager or DD OS CLI, the user will appear in the DDMC list of available users to be added for DD Boost data access and/or Tenant self-service.

For more information about creating a user with DD System Manager, see the *DD OS Administration Guide*. For creating a user with the DD OS CLI, see the *DD OS Command Reference Guide*.

Using DDMC to administer SMT

In DDMC, Secure Multi-Tenancy (SMT) is administered by selecting **Administration > Multitenancy**. SMT is supported on DDVE 3.0 and later.

Controls

In the upper left are controls to Add (green +), Edit (yellow pencil), and Delete (red X) Tenants and/or Tenant Units (depending on what is selected in the tree), and a Tenant (Unit) Details (blue i) icon that displays the Tenant (Unit) Details Lightbox (depending on what is selected). You can also right-click each node in the tree to perform these functions. RBAC (role-based access control) controls all of these actions.

All Tenants tree

Below the controls is the Tenant *tree*, from which you can create and manage Tenants, Tenant Units, and provisioned storage.

The All Tenants node is always displayed and lets you create Tenant objects.

Each node has a control to its left, indicating its Warning or Offline status. This status rolls up to the Tenant and All Tenant nodes. Also, controls for creating, editing, or deleting states are displayed while each operation is in progress. Some actions may not be allowed, depending on the different state or status of the nodes. If there are Tenant Units under a Tenant with the same name, an information icon is displayed for the Tenant node.

The Unmanaged node is displayed only if there are unmanaged Tenant Units available. The only actions that are allowed on the Unmanaged node and Unmanaged Tenant Units are *Add all to Tenant* and *Add to Tenant*, respectively, and these actions are available only through the right-click context menus.

The user can click "Unmanaged", and then, in the right pane can select all tenant-units or single/multiple tenant-unit(s) to add to Tenant. The user then clicks the link "Add to Tenant" to add selected tenant-unit(s) to tenant.

Summary area

At the right is a summary.

When All Tenants is selected, the summary shows the total number of Tenants, Tenant Units, and host systems. You can see if any of the Tenants or Tenant Units are offline or have configuration problems in different severity panels. You can also see the number of unassigned Tenant Units.

When you select a Tenant or Tenant Unit, the summary includes (depending on the item) the name, status, administrator name and email, host systems, data center location, alerts, and MTree and storage information, DD Boost Users, Tenant Self-Service information, and Report schedule and recipients.

Configuration problems

Tenants can be configured directly on Data Domain and PowerProtect systems. This may lead to Tenant name and ID conflicts when these systems are managed by DDMC. DDMC lets you resolve Tenant conflicts by either consolidating the Tenants into one or separating the Tenants with unique names and IDs.

 **NOTE:** Tenants cannot be edited or resolved if any of the systems are in an offline state or cannot be reached over the network.

Generating reports, looking at health, changing locations

To generate reports about Tenants or individual Tenant Units, select **Reports > Management**.

To see the general health for Tenants and Tenant Units, select **Health > Status**, **Health > Alerts**, and/or **Health > Jobs**.

To change a Data Center Location, select **Administration > Properties** and edit the Data Center property. Each Data Domain system must be explicitly assigned a value for Data Center in **Administration > Systems**. If a system has a Data Center property that is assigned, it is grouped under *All* in the Create Tenant Unit wizard.

Storage administrator tasks in Secure Multi-Tenancy

Storage administrators are the *landlords* for backup operators (*tenants*), in an Secure Multi-Tenancy (SMT) environment. Storage administrators install and configure system hardware and software and use DDMC to provision and assign storage to the Tenants that they support.

Storage administrators in an SMT environment perform the following tasks:

- Migrate users from multiple small systems to one or more larger systems
- Isolate each Tenant's data from other Tenants who share storage on the same physical system
- Monitor and manage the space usage and performance of each system
- Monitor and manage the space usage by and the performance that is provided to each Tenant, which ensures that the storage administrator meets the requirements of the service level agreement with each Tenant
- Grouped Tenants with similar characteristics on the same physical system to gain more cross deduplication
- Charge Tenants based on their space usage

Backup operator tasks in Secure Multi-Tenancy

Backup operators are the *tenants* in a Secure Multi-Tenancy (SMT) environment. Backup operators are responsible for scheduling and managing backups and replication for their organization or department using the storage available in their Tenant Units.

Backup operators in an SMT environment perform the following tasks:

- Monitor the performance and resources of their Tenant Units
- Monitor replication
- Generate reports

Creating and managing Tenants

DDMC provides many options for creating and managing Tenants.

Creating Tenants

You can create Tenants from the Multi-Tenancy page.

Steps

1. Select **Administration > Multi-Tenancy**.
2. Highlight **All Tenants** in the tree, and select Add Tenant (green plus sign) above the tree.

3. In the Create Tenant dialog box, type the following information:
 - For **Tenant name** [which is required, as indicated by the asterisk (*)], you can use the name of the client or organization that will use the storage. For example, if you are a service provider, the name might be **XYZ Widget Corp**. If you are a storage administrator for an organization, the name might be **Finance Department**.
 - For **Administrator name** (which is optional), type the name of the backup administrator.
 - For **Administrator email** [which is required, as indicated by the asterisk (*)], type the email address of the backup administrator. This information is used to create a default Alert Notification list.
4. Select **Create**.

Results

The new Tenant appears in the tree.

Viewing Tenant information and status

You can view information about all Tenants or individual Tenants from the Multi-Tenancy page.

Steps

1. Select **Administration > Multi-Tenancy**.
2. Highlight **All Tenants** to see an overview of the configured Tenants, important messages, and the status of multitenant reporting.
3. Highlight a specific Tenant to see the backup administrator's name and email address, important messages about the Tenant Units for this Tenant, and information about reports for this Tenant.
4. For much more detail about the Tenant, select Tenant Details (the blue *i*), above the list of Tenants, to see all of the available information about the Tenant. The *Tenant Details lightbox* is described in the next section.

Tenant Details lightbox

The Tenant Details lightbox provides detailed operating information about a specific Tenant.

The Tenant Details lightbox is accessed from the **Administration > Multi-Tenancy**, using the **Tenant Details** control.

The **Overview** page has the following sections:

- **Tenant**, which includes Tenant name, Administrator, Administrator email, Tenant Units, and Systems.
- **Health**, which includes four LEDs for Alerts, File Systems, DD Boost, and Replication. These alerts can be in a Normal, Warning, or Error state. You can hover over an alert to get more information. The Tooltip on the LEDs lists the Tenant Units that have problems, along with a link to launch the related system for that Tenant Unit. Health LEDs can also be in a disabled state if the underlying component (that is, Replication, DD Boost, and so forth) is either not licensed or disabled on any of the systems of the Tenant.
- **Capacity**, which includes a capacity meter that shows the current utilization, aggregate values for quota available, quota that is used, quota used % (based on all configured MTrees owned by the Tenant), and a warning/error banner, if any of the quotas has not been enabled or configured.
- **Replication**, which includes counts for both automatic and on-demand replication pairs: total, with errors, and with unknown status.
- **Network Bytes Used**, which includes the total, backup, and restore replication bytes used.

The **Capacity** page shows Capacity Overview details with a variable meter that shows the quota (available, used, and used percentage). The Logical Space Usage chart shows plots for Pre-comp that is used for a selected time (24 Hours, 7 Days, 30 Days, 90 Days, or Custom – to set your own time period). There is also a list of Tenant Units that are associated with this Tenant with their MTrees or Storage Units, including a severity panel with any warnings for the MTree/Storage Unit selected.

The **Replication** page shows Replication Overview details that include the total number of bytes replicated for Automatic Replication Pairs and On-Demand Replication Pairs. The Replication Trend chart shows plots for Pre-comp replicated, Post-comp replicated, and/or Compression ratio plots for a selected time (24 Hours, 7 Days, 30 Days, 90 Days, or Custom – to set your own time period).

The **Network** page shows Network Overview details that include the last 24 hours of back-up, restored data, and total inbound and outbound replication. The Trend Analysis charts show plots for Total Network Used, Backup and Restore Bytes Used, and Replication Bytes Used for a selected time (24 Hours, 7 Days, 30 Days, 90 Days, or Custom – to set your own time period).

The **System Charts** page shows the system charts for the system of a selected Tenant Unit that is associated with this Tenant. Desired charts can be added to the chart area (at the right) by enabling the respective checkboxes. You can display Resource charts for CPU utilization and Network throughput; File system charts for Stream counts, Protocol processing, and Protocol throughput. Replication charts for Inbound/Outbound characteristics and Throughput for each type of replication. In the chart area, multiple charts are displayed vertically according to the selection. All of these charts can be displayed for a selected time (24 Hours, 7 Days, 30 Days, 90 Days, or Custom – to set your own time period).

Editing Tenant information

You can change Tenant names, administrator names, and administrator email addresses using the Edit Tenant dialog.

About this task

You may need to *Resolve Tenant Conflicts* If you are managing Tenants from both DDMC and the DD OS CLI. Tenants have two identifiers: their name and a Universally Unique ID (UUID). From the DD OS CLI (starting in 5.7), you can easily create two Tenants with the same name but different UUIDs. DDMC detects this and offer to either merge the two Tenants (by giving them a newly created UUID) or rename one of the Tenants. When done, no Tenants will share a name without also sharing a UUID (and conversely).

If you change the name of a Tenant that is part of a PCM schedule, the name change is not updated automatically in the schedule. You must manually add the new Tenant name to the PCM schedule.

Steps

1. Select **Administration > Multi-Tenancy**.
2. In the tree, select the Tenant that you want to update, and select Edit Tenant (yellow pencil) above the tree.
3. In the Edit Tenant dialog, edit what you need to change, and select **Save**.

Results

The edited Tenant will again be displayed in the tree.

Deleting Tenants

When you no longer need to provide storage for an organization, you can delete the Tenant that corresponds to that organization.

Steps

1. Select **Administration > Multi-Tenancy**.
2. Highlight the Tenant in the tree, and select Delete Tenant (red X) above the tree.
3. In the Delete Tenant dialog box, you have two options:
 - **Remove all Tenant Units**, which will preserve the data, so that the Tenant Unit may be assigned to another Tenant. The Tenant Units will be moved to the **Unmanaged** Tenant Unit pool and will retain all MTrees/Storage Units associated with them.
 - **Destroy all Tenant Units**, which will destroy all of the Tenant Units and any MTrees and Storage Units associated with them.
4. Select **Yes**.

 **NOTE:** Deleting a Tenant cannot be *undone* from DDMC, so be very careful when performing this task.

Results

The Tenant has been deleted from the tree.

What to do if delete Tenant fails

When you try to delete a Tenant, the operation may fail for a variety of reasons.

First, go to the **Health > Jobs** page, select the failed job, and observe the reason for the failure, which may include:

- The file system of one or more of the Data Domain or PowerProtect systems under the Tenant is turned off.

- Some of the Data Domain systems under the Tenant are not reachable or are powered off.
- The DD Boost feature of one or more of the systems under the Tenant is disabled or is not licensed.

You can manually fix these problems using both the DD System Manager and the DDMC command line interfaces (you need to fix them in both places, as they are Data Domain system-related). Then, you can try to delete the Tenant again using DDMC.

Creating and managing Tenant Units

DDMC provides many options for creating and managing Tenant Units.

Creating a Tenant Unit with the wizard

You can create a Tenant Unit with the Create Tenant Unit Wizard.

Prerequisites

Storage for a Tenant is contained within a virtual partition that is called a *Tenant Unit* on a Data Domain or PowerProtect system. To assign storage to a Tenant, you can use the *Create Tenant Unit Wizard* to create the Tenant Unit, provision storage, and assign the Tenant Unit to a Tenant. You can also create an empty Tenant Unit for a Tenant and provision storage later.

Select **Administration > Multi-Tenancy**. Then select a Tenant, and the **Add** (green +) control.

You have three choices when creating a Tenant Unit:

- **Create a Tenant Unit with manual provisioning**, where you create/select the MTrees and Storage Units that are associated with this Tenant Unit. You can also optionally create DD Boost Data Access users to go with the Storage Units.
- **Create a Tenant Unit with automatic provisioning**, where you can add new or existing DD Boost Data Access users to this Tenant Unit. This allows backup software to create Storage Units that are assigned to this Tenant Unit.
- **Create an empty Tenant Unit**, where you can provision the Tenant Unit later using the Edit Tenant Unit dialog box.

Steps

1. On the first page of the wizard, Identify Host System:
 - For **Datacenter location** (which is optional), select a location. These locations (for example: Dallas, New York) must have been entered previously as Data Center location properties. (**Administration > Properties > Data Center**).
 - For **Size now (GiB)** (which is optional), type a number to filter systems that do not currently have sufficient storage capacity.
 - For **Size to grow (GiB)** (which is optional), type a number to filter systems that will not have sufficient capacity at a specified time in the future (set in the next field, "Time to grow"), based on capacity projections. The size to grow is actually *the size to grow to by the specified time*. For example, for a specified time of 6 months, if the size now is 1 GiB, and the size to grow is 2 GiB, in 6 months, the minimum capacity requirement would be 2 GiB.
 - For **Time to grow** (which is optional), type the time after which the "Size to grow" amount of capacity should be reached.
2. On the second page of the wizard, Select Host System, you see systems that have enough logical capacity to host the Tenant Unit:

How do I check host system performance? Use the following information to determine the best system on which to create the Tenant Unit.

- **Available now** indicates systems that you can select now.
- **Available in 6 months** is displayed if you selected 6 months in the "Time to grow" field on the previous page, or did not explicitly select a value. **Available in 12 months**, **Available in 18 months**, or **Available in 24 months** is displayed if you selected those values in "Time to grow". For example, for a specified time of 6 months, if the size now is 1 GiB, and the size to grow is 2 GiB, in 6 months, the minimum capacity requirement would be 2 GiB. Any system that has a lower projected capacity is filtered from the list. Also, any system offline at the time, as well as any collection destination system, is filtered from the list. Also, any systems running a version prior to DD OS 5.6 are filtered from the list, that is, only systems running DD OS 5.6 or later are listed.
- **Existing Tenant Units** displays the current number of Tenant Units on this system.
- For systems with an information (blue *i*) control, you can hover to see a warning message explaining why a projection cannot be made.
- If a system is not listed, it may be because it:

- is not in the specified data center.
- is offline.
- is running DD OS 5.6 or earlier.
- has insufficient capacity.
- has a replication destination.
- is a system for which you do not have administrative privileges.
- For the selected system, the charts at the bottom show historical data, including **Throughput** for the selected connection Port, **CPU** utilization for each system, and **Stream Count**. You may toggle the Port and the time (Last 7 days, Last 30 days, or Last 90 days) drop-down menus to get different sets of data.

3. On the third page of the wizard, Administration, type name and administrator details:

- For **Tenant Unit name** [which is required, as indicated with the asterisk (*)], type a unique Tenant Unit name per system.
- For **Administrator name** (which is optional), type the name of the backup administrator.
- For **Administrator email** [which is required, as indicated with the asterisk (*)], type the email address of the backup administrator. This is used to create a default Alert Notification list.
- When **Create an Empty Tenant Unit** is selected, **Use strict security mode** options will now show.
- Check **Use strict security mode** if you want to allow incoming replications only if they are from another Tenant Unit that is owned by the same Tenant.
- Select or type **Management IP Addresses** (which is optional), as needed.

i **NOTE:** See the following section, [Security mode and management IP addresses](#) on page 73, for more about these topics.

4. The fourth page of the wizard depends on the previous choice. [Note that for "Create an empty Tenant Unit", you will go to the final page (step 5).]

a. For manual provisioning, you can create MTrees/Storage Units.

- MTrees/Storage Units can be added here, when creating a Tenant Unit with Manual Provisioning. You can also add them when editing a Tenant Unit.
- You can add new MTrees or Storage Units, or select from the Existing MTrees or Storage Units on the host system.
- You can also edit, unassign, or destroy MTrees or Storage Units from the same area.
- If an MTree or Storage Unit selection is disallowed, you can hover the mouse over it, to see more information.

b. For automatic provisioning, you can configure users for data access over the DD Boost protocol.

- You can add an existing local user or create a new local user and promote the local user to DD Boost user.
- You can delete the selected DD Boost User.
- The table contains DD Boost Data Access User names and the Storage Units count associated with the user.
- The information panel shows when one or more users are selected.
- The configuration is not changed until you select Create on the Summary page.
- If there are one or more local users in the list, the first local user in the list is selected by default. If there are no local users in the list, the "New local user" is selected. All selected users or newly created users will automatically be default Tenant Units.
- A warning shows if the current selected local user already has another Tenant Unit as their default Tenant Unit.
- The first entry in the "Local user" drop-down list is "New local user", which lets you create a new local user and add it as a DD Boost Data Access user.
- When selecting "New local user", the Add Data Access User dialog box changes to a **Add New Data Access User** form.

5. The fifth (final) page (fourth page for "Create an empty Tenant Unit") of the wizard is a Summary, showing data from the previous pages.

- The Tenant Unit is not created until you select Create.
- You have the option to send an email to the Tenant Unit administrator on the successful creation of the Tenant Unit.
- Creating a Tenant Unit with any sort of provisioning (not empty) automatically generates a pair of Report Templates (Status and Usage) and schedule them.
- You may get one of two warnings: (1) You have not provisioned this Tenant Unit correctly. Add MTrees or Storage. (2) You have not provisioned this Tenant Unit correctly. Make this Tenant Unit the Default Tenant Unit for one of the DD Boost Data Access Users.

Results

The newly created Tenant Unit is added to the tree.

What to do if create Tenant Unit fails

Creating a Tenant Unit may fail for a number of reasons.

It may fail for simple reasons such as a duplicate Tenant Unit name, or it may fail if there are sudden system state changes, such as a network/connectivity issue.

Within the create process itself, there may be failures where MTrees or Storage Units may fail to get created for one or more reasons, or DD Boost users may not get created.

Creating a Tenant Unit will succeed even if the configuration of an individual component like MTrees or DD Boost users fails. So, the final components of a newly created Tenant Unit might not match the specifications.

To see the success and/or failed information for each task, or if there is an inconsistency in what you expected and what was created, select **Health > Jobs** to see additional messages.

You must address the reasons for failure before trying to re-create a new Tenant Unit, or you risk seeing the same failure situations again.

Security mode and management IP addresses

Strict Security Mode assures that incoming replication is from another Tenant Unit that is owned by the same Tenant. Also, this mode must be enabled to allow management connections to or from assigned IPs. *Management IP addresses* let you associate a Tenant Unit with certain IP addresses for both remote clients and other local DDMC systems.

About this task

- *Remote client addresses* are IP addresses from which incoming connections will be accepted. These addresses must be IPv4 or IPv6.
- *Local DDMC addresses* are IP addresses that are available to connect to and manage this Tenant Unit. You can enter new addresses that will be configured on the Data Domain system. Or you can select from configured IPv4 or IPv6 addresses on the Data Domain system that are not assigned to other Tenant Units. (Assigned IP addresses are unavailable and cannot be selected.)

Viewing Tenant Unit information and status

You can view information about all Tenant Units from the Multi-Tenancy page.

Steps

1. Select **Administration > Multi-Tenancy**.
2. Select a Tenant Unit in the tree to view a summary page and critical alerts.
3. For more detail about the Tenant Unit, select Tenant Unit Details (the blue i), above the tree, to see all of the available information about the Tenant Unit. The *Tenant Unit Details lightbox* is described in the next section.

Tenant Unit Details lightbox

The Tenant Unit Details lightbox provides detailed operating information about a specific Tenant Unit.

The Tenant Unit Details lightbox can be accessed from the **Administration > Multi-Tenancy, Health > Status**, or **Health > Alerts** page (Tenants View), using the **Tenant Unit Details** control.

The **Overview** page has the following sections:

- **Tenant Unit**, which includes Tenant Unit name, Administrator, Administrator email, Host System, and Data Center Location.
- **Health**, which includes four LEDs for Alerts, File Systems, DD Boost, and Replication. These alerts can be in a Normal, Warning, or Error state. You can hover over an alert to get more information. Health LEDs can also be in a disabled state if the underlying component (that is, Replication, DD Boost, and so forth) is either not licensed or disabled for the system of the selected Tenant Unit.
- **Host System Performance Details**, which shows data flow for Throughput, CPU and Stream Count. Different network ports can be selected. Chart durations can be selected among: Last 24 Hours, 7 Days, 30 Days, 90 Days, and Custom.

- **Capacity**, which includes a capacity meter that shows the current utilization, aggregate values for quota available, quota used, quota used % (based on all configured MTrees owned by the Tenant Unit), and a warning/error banner, if any of the quotas has not been enabled or configured.
- **Replication**, which includes counts (inbound and outbound) for both automatic and on-demand replication pairs: total, with errors, and with unknown status.
- **Network Bytes Used**, which includes the total, backup, and restore replication bytes used.

The **Capacity** page shows Capacity Overview details with a variable meter that shows the quota used percentage; a Logical Space Usage chart that can be scaled to view certain periods of usage; and a list of Tenant Units with their MTrees or Storage Units, including a severity panel with any warnings for the MTree/Storage Unit selected.

The **Replication** page shows Replication Overview details that include the total number of bytes replicated for Automatic Replication Pairs and On-Demand Replication Pairs. The Replication Trend chart shows at least one of: Pre-comp replicated, Post-comp replicated, and Compression ratio plots in a customized time plot.

The **Network** page shows Network Overview details that include the last 24 hours of back-up, restored data, and total inbound and outbound replication. The Trend Analysis shows charts that can be viewed for a certain period by selecting one of the four options (24 Hours, 7 Days, 30 Days, 90 Days) or by selecting Custom, which lets you select a different time frame.

The **System Charts** page shows the system charts for the system of the selected Tenant Unit. Desired charts can be added to the chart area (at the right) by enabling the respective checkboxes. You can display Resource charts for CPU utilization and Network throughput. File system charts for Stream counts, Protocol processing, and Protocol throughput; Replication charts for Inbound/Outbound characteristics and Throughput for each type of replication. In the chart area, multiple charts are displayed vertically according to the selection.

Editing Tenant Unit information

You can change all types of information for both managed and unmanaged Tenant Units using the Edit Tenant Unit dialog.

Steps

1. Select **Administration > Multitenancy**.
2. Highlight the Tenant Unit in the tree, and select Edit Tenant Unit (yellow pencil) above the tree.
3. The Edit Tenant Unit dialog has the following tabs: General, Alert Notifications, DDBoost Data Access Users, MTrees, and Tenant Self-Service, which are described in the following sections.

Editing Tenant Units: General tab

You can change administrative information for both managed and unmanaged Tenant Units using the General tab in the Edit Tenant Unit dialog.

Steps

1. Select **Administration > Multitenancy**.
2. Highlight a Tenant Unit in the tree, and select Edit Tenant Unit (yellow pencil) above the tree.
3. In the General tab, you can change the following:
 - Tenant Unit name
 - Administrator name
 - Administrator email – If the administrator email is modified, report templates sending reports associated with the Tenant Unit to that administrator need to be re-routed. After editing the administrator email, a popup appears confirming whether a change needs to be made for all report templates associated with the old email. If you select Yes, all old administrator emails will be replaced with the new value.
 - Security Mode – You can choose to enable *strict security mode*, which assures that any incoming replication is from another Tenant Unit owned by the same Tenant. In addition, this mode must be enabled to allow management connections to or from assigned IPs.
 - Management IP Addresses – You can add or delete management IP addresses for remote client addresses and/or local DDMC addresses.

Editing Tenant Units: Alert Notifications tab

Each Tenant Unit has a default alert notification list (created by the Data Domain or PowerProtect system) containing the administrator email. You can create new alert notification lists, edit existing lists, or delete lists associated with the Tenant Unit, using the Alert Notifications tab in the Edit Tenant Unit dialog.

Steps

1. Select **Administration > Multitenancy**.
2. Highlight a Tenant Unit in the tree, and select Edit Tenant Unit (yellow pencil) above the tree.
3. In the Alert Notifications tab, select Add (green plus sign).
4. In the Add Alert Notification Group dialog, enter a name for the notification group.
5. Select Add (green plus sign), and enter the first email address.
Optionally, continue selecting Add to enter more addresses.
6. Select **Add** at the bottom of the dialog when you have finished adding addresses, and then select **OK** or **Apply** to save your changes.

Editing Tenant Units: Data Access Users tab

Data Access Users are users that are configured for specific Tenant Units (one or more user per Tenant Unit). You can optionally designate a Tenant Unit as the default Storage Unit for a Data Access User. When your backup software creates new Storage Units for a user, the software automatically uses the default Tenant Unit.

Steps

1. Select **Administration > Multitenancy**.
2. Highlight a Tenant Unit in the tree, and select Edit Tenant Unit (yellow pencil) above the tree.
3. In the Data Access Users tab, add, edit, or delete users, as desired. New Data Access users are assigned the role of *none*. If a user has already been created with a role other than none, that user is disabled and can only be deleted from the table. Also, if a user has already been associated with multiple Tenants, that user is disabled and can only be deleted from the table. Password validation for a new local user is based on the DD OS password policy strength associated with the current Tenant Unit.
4. The columns indicate:
 - **MTrees Accessed** - The combined total of Storage Units and vDisk Pools.
 - **MTree Type** - Supported types are Storage Unit and vDisk Pool. If a user is not associated with an MTree's access, the MTree type will be None.
5. Select **OK** or **Apply** to save your changes.

Fixing a Double Agent issue

Double Agent data access users are users associated with more than one tenant.

About this task

If a local user owns multiple Storage Units, and the Tenant Units that contain those Storage Units do not all belong to the same Tenant, this is definitely a misconfiguration and always results in a security breach (either data or administrative isolation is violated). This situation can also result in Tenant usage report errors.

The effects of the misconfiguration depend on which Tenants actually own the data in the affected Storage Units. If the data in all of these Storage Units is actually owned by a single Tenant, then there is no data isolation security breach (each Tenant can access only their own data), but the usage reports for the Tenants will be incorrect. Some Tenants will see usage for Storage Units that belong to other Tenants, and some Tenants will not see usage for some of their Storage Units. In addition, some Tenants will be able to view the Storage Unit names and usage of other Tenant's Storage Units. So this is also an administrative isolation security breach.

If some Storage Units contain data for one Tenant, and other Storage Units contain data for a different Tenant, then different Tenants have been given the same user credentials to access their Storage Units, so there is a data isolation security breach, since each Tenant can access the other Tenant's data in the Storage Units owned by the shared local user. However the usage reports for each Tenant will be correct in this case.

Fixing a user not "none" issue

Data access users must always have the role of *none* .

About this task

A user who does not have a role of *none* is already associated with a Tenant. Thus, the user credentials (user/password) of a user who has permission to view and possibly even change the configuration/data on the system have been given to a Tenant. If the user has the *admin* role, for example, the Tenant can now access (read/write) any other Tenant's data, and view/change any system configuration.

This security breach is present whether this (non-*none* role) user is associated with just one Tenant, or multiple, different Tenants. The main security breach is not that one user is used by multiple Tenants; it is that a user given to a Tenant for use can view and/or modify configuration and data that does not belong to the Tenant.

To prevent security breaches, data access users must *always* have a role of *none*. In some customer configurations where Tenants are considered trustworthy, Tenants may have some non-*none* role users, but the best security practice is to not allow this.

Fixing a user not "none" and a Double Agent issue

You may sometimes have cases in which a data access user *both* does not have the role of *none* and is a *Double Agent* user, which is a user associated with more than one Tenant. You must resolve both of these issues before continuing.

About this task

A user who does not have a role of *none* is already associated with a Tenant. Thus, the user credentials (user/password) of a user who has permission to view and possibly even change the configuration/data on the system have been given to a Tenant. If the user has the *admin* role, for example, the Tenant can now access (read/write) any other Tenant's data, and view/change any system configuration. (See the previous section, [Fixing a user not "none" issue](#) on page 76, for more on this problem.)

A *Double Agent* user may own multiple Storage Units, but the Tenant Units that contain those Storage Units do not all belong to the same Tenant. This is definitely a misconfiguration and always results in a security breach (either data or administrative isolation is violated). This situation can also result in Tenant usage report errors. (See the previous section, [Fixing a Double Agent issue](#) on page 75, for more on this problem.)

Editing Tenant Units: DD Boost Streams tab

You can limit the number of streams an application can use when reading or writing data to a Storage Unit. If a client uses more than the set limit, an alert will be generated by the Data Domain system.

Steps

1. Select **Administration > Multitenancy**.
2. Highlight a Tenant Unit in the tree, and select Edit Tenant Unit (yellow pencil) above the tree.
3. In the DD Boost Streams tab, view the Storage Units associated with this Tenant Unit.
4. If you want to set limits for a Storage Unit, select that unit, and then select **Set Limits**.

Configuring DD Boost stream limits

You can configure stream warning limits for each Storage Unit for four items: Read, Write, Replication, and Combined. When any of these stream counts exceeds the warning limit, an alert is generated.

Steps

1. Select **Set Limits** from the **DDBoost Streams** tab of the **Edit Tenant Unit** dialog [which you can get to by selecting **Administration > Multi-Tenancy**, then selecting a Tenant Unit and Edit Tenant Unit (yellow pencil)].
2. In the Set DDBoost Stream Limits dialog, enter values for the Read, Write, Replication, and Combined stream limits. Do not exceed the DD system limits. Also note that a single value cannot be larger than the combined limit.

For hard limits there are two additional validation rules:

- The combined limit is also no greater than the sum of the other hard limits (if it is, you will hit one of the other limits first and never the combined limit).
 - The combined limit is less than the maximum individual hard limit (if it is, you will never hit that individual limit, that is, you will always hit the combined limit first).
3. If the limits are surpassed, an alert will be generated by the system.
 4. Select Set.

Editing Tenant Units: MTrees tab

You can create and manage MTrees, Storage Units, vDisk Pools, and VTL Pools using the MTrees tab in the Edit Tenant Unit dialog. In addition to this method, you can also add these when you are creating a Tenant Unit with Manual Provisioning.

Steps

1. Select **Administration > Multitenancy**.
2. Highlight a Tenant Unit in the tree, and select Edit Tenant Unit (yellow pencil) above the tree.
3. In the MTrees tab, add, edit, or delete MTrees, Storage Units, vDisk Pools, and VTL Pools, as desired.

NOTE: vDisks with *double agent* data access users (that is, users associated with another Tenant) or users with a role other than *none* cannot be associated with the Tenant Unit.

4. If capacity quota is enabled on the host system, you may edit soft and hard quotas.

Adjusting soft/hard quotas for MTrees and Storage Units

Quotas can be enabled or disabled on a host system using the command line interface (CLI) or with DD System Manager. You cannot enable or disable quotas using DDMC. You can *adjust* quotas using DDMC if the host system quotas have already been enabled.

Prerequisites

The host system quotas must have already been enabled.

Steps

1. Select **Administration > Multitenancy**.
2. Highlight the Tenant Unit in the tree, and select Edit Tenant Unit (yellow pencil) above the tree.
3. In the MTrees tab, highlight a Storage Unit or MTree in the list, and select Edit (yellow pencil).
4. Set the desired quota values in the Edit MTree or Edit Storage Unit dialog, and select **Save**.
5. Select **OK** or **Apply** to save your changes.

Next steps

You can also enable or disable quotas on the host system by:

1. Launch the DD System Manager for the specific Data Domain or PowerProtect system from DDMC.
2. Select **Data Management > Quota tab**.
3. Enable or disable quotas, as needed.

You can also enable or disable quotas using the CLI. See the *DD OS Command Reference Guide*.

Editing Tenant Units: Tenant Self-Service tab

Tenant Self-Service is a method of letting a Tenant log in to a Data Domain or PowerProtect system to perform some basic services (add, edit, or delete local users, NIS groups, and/or AD groups). This reduces the bottleneck of always having to go through an administrator for these basic tasks. The Tenant can access only their assigned Tenant Units. Tenant Users and Tenant Admins will, of course, have different privileges.

About this task

To create a list of users that may have Self-Service access to a particular Tenant Unit:

Steps

1. Select **Administration > Multitenancy**.
2. Highlight a Tenant Unit in the tree, and select Edit Tenant Unit (yellow pencil) above the tree.
3. In the Tenant Self-Service tab, you must first enable Tenant Self-Service, if it disabled (which is it by default).
4. Note that in this table:
 - The **Type** column displays management-user or management-group.
 - The **Group Type** column displays either NIS or Active Directory for groups, and N/A for users.
 - The **Role** column displays tenant-admin or tenant-user.
5. To add a self-service user, select Add (green plus sign). In the Add Self-Service User dialog, select the desired local user, NIS group, or AD group, or create a new local user (there is no default). If you select New local user, the dialog will add fields for Name, Password/Confirm, and Role (tenant-admin or tenant-user). Password validation for a new local user is based on the DD OS password policy strength associated with the current Tenant Unit.
6. To edit a self-service user, select a User or Group, and select Edit (yellow pencil). You can change the Role from tenant-admin to tenant-user, or vice-versa.
7. To delete a self-service user, select a User or Group, and select Delete (X). You will get a confirmation dialog to make sure that you definitely want to delete this user or group. A new Tenant self-service user or group is assigned the role of *none*. If a user or group has already been created with a role other than *none*, that user or group is disabled and can only be deleted from the table. Also, if a user or group has already been associated with multiple Tenants, that user or group is disabled and can only be deleted from the table.

Deleting Tenant Units and unassigning provisioned storage

You can delete Tenant Units, and if a Tenant Unit has provisioned storage, you can unassign that storage to be reassigned later to another Tenant Unit, or you can destroy all of the data. *Be very careful* when performing this task – it cannot be undone.

Steps

1. Select **Administration > Multitenancy**.
2. Highlight a Tenant Unit in the tree, and select Delete Tenant Unit (red X) above the tree.
3. In the Delete Tenant Unit dialog, if the Tenant Unit has provisioned storage, you have two options:
 - **Unassign all storage**, which retains all MTrees and Storage Units associated with the Tenant Unit, so they can be reassigned later to another Tenant Unit.
 - **Destroy all storage**, which deletes all MTrees and Storage Units associated with the Tenant Unit.
4. Select **Yes** to delete the Tenant Unit.
5. Observe that the Tenant Unit has been deleted from the tree.

What to do if delete Tenant Unit fails

When you try to delete a Tenant Unit, the operation may fail for a variety of reasons.

First, go to the **Health > Jobs** page, select the failed job, and observe the reason for the failure, which may include:

- The file system of the system on which the Tenant Unit resides is turned off.
- The Data Domain system on which the Tenant Unit resides is not reachable or is powered down.
- The DD Boost feature of the system on which the Tenant Unit resides is disabled or is not licensed.

You can manually fix these problems using both the DD System Manager and the DDMC command line interfaces (you need to fix them in both places, as they are system-related). Then, you can try to delete the Tenant Unit again using DDMC.

Adding an unmanaged Tenant Unit to a Tenant

Working from the DD OS CLI (command-line interface), administrators can create Tenant Units without adding them to tenants. These Tenant Units are referred to as *unmanaged*. In DDMC, you cannot create an unmanaged Tenant Unit, but you can add an unmanaged Tenant Unit to a tenant.

Steps

1. Select **Administration > Multitenancy**.
2. Select the Unmanaged node in the tree. A table is displayed on the right, which contains all unmanaged Tenant Units and the host systems on which they reside.
3. To add all unmanaged Tenant Units to a Tenant, right-click the Unmanaged node, and select Add all to Tenant. In the Add (All) Tenant Units dialog, select the Tenant name, and select Add.
4. If you want to add only a specific Tenant Unit or Units to a Tenant, go back to the table to select the checkbox or checkboxes next to them. Or to select a single Tenant Unit, and see a summary about it, you can expand the **Unmanaged** list (if it is not already expanded), and select a single Tenant Unit.
5. At the top right, select the **Add to Tenant** link.
6. In the Add Tenant Unit(s) dialog, select a Tenant name, and select **Add**. The Tenant Unit will be moved from the Unmanaged node to the selected Tenant, in the tree.

Next steps

You may encounter a potential conflict when trying to assign a Tenant Unit.

Suppose you have a DD Boost user, or Tenant self-service user, configured under a current unmanaged Tenant Unit. If the same user is configured to the managed Tenant Unit of Tenant T2, but you want to assign the Tenant Unit to Tenant T1, this is considered a conflict and is not allowed.

Creating, editing, and generating SMT reports

You can create, edit, and generate reports for Secure Multi-Tenancy (SMT) using DDMC.

SMT report permission table

Permissions for working with creating and viewing reports for Tenants and Tenant Units depend on the role of the user in both DDMC and on the DD OS.

Table 12. Permission table for Tenants and Tenant Units, DDM admin and limit-admin

DDMC user/DD OS role	DDMC admin/DD OS sysadmin	DDMC limited-admin/DD OS sysadmin
Report Template		
View all report templates	yes	yes
View Tenant report configuration information in summary page	yes	yes
View Tenant Unit report configuration information in summary page	yes	yes
Create Auto Tenant report template	yes	yes
Create Auto Tenant Unit report template	yes	yes
Create Manual Tenant report template	yes	yes
Create Manual Tenant Unit report template	yes	yes

Table 12. Permission table for Tenants and Tenant Units, DDM admin and limit-admin (continued)

DDMC user/DD OS role	DDMC admin/DD OS sysadmin	DDMC limited-admin/DD OS sysadmin
Maintain and tag SMT report template configuration	yes	yes
Delete/destroy MTree-related reports	yes	no

Table 13. Permission table for Tenants and Tenant Units, DDMC user

DDMC user/DD OS role	DDMC user/DD OS sysadmin	DDMC user/DD OS user or backup operator	DDMC user/no DD OS role
Report Template			
View all report templates ^a	no	no	no
View Tenant report configuration information in summary page ^b	no	no	no
View Tenant Unit report configuration information in summary page	yes	yes	no
Create Auto Tenant report template	no	no	no
Create Auto Tenant Unit report template	yes	yes	no
Create Manual Tenant report template ^c	no	no	no
Create Manual Tenant Unit report template	yes	yes	no
Maintain and tag SMT report template configuration ^d	yes	yes	no
Delete/destroy MTree-related reports	no	no	no

- a. DDMC *user* can view only templates or reports that they created.
- b. Only DDMC *admin* should be allowed to create Tenant report template.
- c. DDMC *user* is not allowed to manually create a Tenant report template.
- d. If the reports of a DDMC *user* are deleted, that user is warned, and the reports are re-created and tagged for that user only.

Creating SMT report templates

Secure Multi-Tenancy (SMT) report templates configure daily status and usage metrics for Tenants and Tenant Units.

About this task

NOTE: If a user who is the "owner" of any report templates is deleted from DD Management Center, those report templates are either assigned to a new owner or deleted. If those templates are assigned to a new owner, the reports will no longer run at their scheduled times.

Steps

1. Select **Reports > Management**.
2. Select Add (green plus sign).
3. In the Add Report Template dialog box, select **Multi-Tenancy Reports** and select **Next**.

4. Type a name, and select a template. The template choices are **Daily Status** or **Usage Metrics**. Choose one or more Sections to include, and select **Next**.
5. Select a Scope (**Tenant Unit** or **Tenant**). The Daily Status report is always configured to show the last 24 hours of historical data, and you can select the Report retention (Forever, 7 days, 30 days, 90 days). The Usage Metrics report (which is generated as an Excel spreadsheet) lets you display data for a full month or a full week. Select **Edit** to set a schedule for the frequency and time the report is run. Report generation time is two hours ahead of *Starts On* time.
6. For the Tenant Unit report template, the Tenant Unit admin email messages are added by default. For the Tenant report template, the Tenant admin email is added by default. You can manually add or remove these email messages.
7. Review the details, and select whether to save the template for later use and/or to run the report immediately. Select **Finish**.

Results

After it has been created, a Multi-Tenancy report template is added as an entry in the reports table. When selected, the template can be used to immediately run a report, or it can be edited or deleted, or the time it was last run can be displayed.

Editing SMT report templates

You can reconfigure an SMT report template using the Edit control. The report's content, schedule, and email distribution can be modified in the template.

Steps

1. Select **Reports > Management**.
2. Select a template, and select Edit (yellow pencil). In the Edit Report dialog, you can select from three tabs.
3. In the **Content** tab, the template name can be renamed and template sections can be re-selected for the report. Note that the template, itself, is not editable.
4. In the **Scope** tab, the template scope and schedule can be changed. The report template can be changed from a Tenant report to a Tenant Unit report or from a Tenant Unit report to a Tenant report. For the daily status report template, the schedule can be changed only to daily time. For the usage report template, the time span can be weekly or monthly. If time span is weekly, only weekly can be scheduled for *start on* time, and if time span is monthly, only monthly can be scheduled for *start on* time. Both daily status and usage report templates can modify the report retention period (Forever, 7 days, 30 days, 90 days).
5. In the **Email** tab, emails can be manually added or removed from the *When report is finished* list or/and from the *If an error occurs* list.
6. Select **Apply** and/or **OK**.

Generating SMT reports

An SMT report can be generated after the last step of the Create Report wizard or by selecting a report template listed in the Template name table and selecting **Run Report**.

About this task

Schedules may be consolidated on multiple Data Domain and PowerProtect systems, as follows:

- If two or more schedules have the same name, type, and schedule (for example, "every Monday at 7 AM"), DDMC displays one schedule that is configured on different systems.
- If two schedules have the same name, but different types and/or different scheduled times, DDMC displays two schedules.
- If a schedule is *Disabled* on one system, but *Enabled* on another, DDMC displays one schedule.

Steps

1. Select **Reports > Management**.
2. Select a report template from the list.
3. Select Run Report.

Results

A report (named by concatenating the timestamp to the template title) is created and opened as a PDF file in the browser, except for the Tenant Usage report, which is generated as an Excel file.

The report generation information is listed in the Report History table, where it can be viewed, renamed, or deleted.

Performing Additional Configuration

Topics:

- [Managing network settings](#)
- [Managing access to DD Management Center](#)
- [Managing general configuration settings](#)

Managing network settings

The **Settings** page presents status and configuration information for network interfaces, DNS, hosts, SNMP, and routes. Settings can be accessed via the gear icon on the DDMC Banner in the upper right corner. Use this area to configure networking for the DDMC.

Configuring network settings

Click the gear icon in the DDMC banner to access **Settings**, then select one of the options under **Network**.

Related concepts

[Configuring network interfaces](#) on page 84

[Configuring routes](#) on page 88

Viewing network settings

You can view network settings for DDMC, while also adding or removing settings.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select one of the options under Network.
2. View the network settings (described in the following table), and use the add, edit, or delete button to change the configuration.

Table 14. Network settings

Item	Description
Hosts	
Mode	Specify whether to use a gateway address from DHCP or a statically configured IP address
Hostname	Hostname of selected Data Domain or PowerProtect system
Domain name	Fully qualified domain name that is associated with selected Data Domain or PowerProtect system
Mapping	Add, edit, or delete hosts that are connected to DDMC
DNS	
DNS servers	Specify whether to use DHCP, or manually add, edit, or delete static IP addresses for DNS servers
Search domain	List of search domains that are used by a system. The system applies the search domain as a suffix to the hostname.
Routes	
Static routes	

Table 14. Network settings (continued)

Item	Description
IPv4 gateway	Specify whether to use a gateway address from DHCP or a statically configured IP address
IPv6 gateway	Specify whether to use a gateway address from DHCP or a statically configured IP address
Static routes	Add, edit, or delete static routes by specifying the interface, destination, and gateway
Dynamic routes	
Dynamic routes	View a list of dynamic routes that are assigned by the system.
SNMP	
Status	Enable or disable SNMP.
Location	Specify the SNMP location
Contact	Specify the SNMP contact
V3 configuration	Add, edit, or delete SNMP V3 users and trap hosts
V2C configuration	Add, edit, or delete SNMP V2C communities and trap hosts

Related concepts

[Managing a domain search list](#) on page 87

[Mapping hosts](#) on page 86

[Configuring DNS settings](#) on page 87

Related tasks

[Configuring hosts](#) on page 85

Configuring network interfaces

You can modify physical network connections and existing interface configurations for DDMC from the **Settings** page.

Related concepts

[Configuring network settings](#) on page 83

[Configuring routes](#) on page 88

Viewing interface information

The Interfaces page (**Settings > Network > Interface tab**) lets you manage and configure the physical (Ethernet) interface, DHCP, DDNS, and IP addresses, and displays network information and status.

There are two parts to this page: the Interfaces area and the Details area. Select an interface and click **Edit** to modify an interface.

Table 15. Interfaces area

Item	Description
Interface	Name of each Ethernet interface that is associated with DDMC. Physical interfaces names start with eth.
Enabled	Lets you view or change status of the interface.
DHCP	Indicates whether the interface is configured with an IP address from a DHCP (Dynamic Host Configuration Protocol) server.
IP Address	IP address that is associated with the interface, which is used by the network to identify the interface. If the interface is configured through DHCP, an asterisk appears after this value.

Table 15. Interfaces area (continued)

Item	Description
Netmask	Netmask that is associated with the interface. Uses the standard IP network mask format. If the interface is configured through DHCP, an asterisk appears after this value.
Link	Indicates whether the physical Ethernet link is active.
Additional Info	Provides additional settings for the interface, for example, the bonding mode.

To populate the Details area, select an interface.

Table 16. Details area

Item	Description
Interface Name	Name of selected interface.
Hardware Address	MAC address of selected interface, for example, <code>00:02:b3:b0:8a:d2</code>
Cable	Indicates whether interface is Copper or optical fiber.
MTU	Maximum Transfer Unit value that is assigned to interface.
Auto Negotiate	Indicates whether interface is enabled to automatically negotiate Speed and Duplex settings. If it is disabled, then Speed and Duplex values are manually set.
Duplex	Protocol that is used with Speed value, which sets data transfer protocol. Values are Unknown, Full, or Half.
Speed	Protocol that is used with Duplex value, which sets rate of data transfer. Values are Unknown, 10 Mb/s, 100 Mb/s, 1000 Mb/s, or 10 Gb/s.
Supported Speeds	Lists all speeds the interface is capable of using.

Configuring hosts

Both the host name and domain name are used by other systems when they want to access DDMC. The host name can be set manually or automatically generated with DHCP.

About this task

Note the following before setting a host or domain name:

- Do not include an underscore in the host name. It is incompatible with some browsers.
- Changing the names of an active host can cause: (1) a break in the current connection – if this happens, log back in, and check the saved settings, and/or (2) disruption of communication with managed systems.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Network > Hosts**.
2. Select how you want to set the host and domain names:
 - **Obtain Settings using DHCP.**
 - **Manually.**
 - Enter a host name.
 - Enter a domain name, which is the domain name associated with DDMC. Typically, this is your company domain name. For example, **yourcompany.com**
3. Click **Apply**.

Related concepts

[Managing a domain search list](#) on page 87

[Mapping hosts](#) on page 86

[Configuring DNS settings](#) on page 87

Related tasks

[Viewing network settings](#) on page 83

Mapping hosts

Use the Hosts Mapping area to add a mapping that ties an IP address to a hostname.

Mapping Hosts is required when DNS is not configured. DNS maps a device's name with its IP address. If DDMC is not configured in DNS (and if the systems are not configured to use DNS), then host mapping is required.

Related concepts

[Managing a domain search list](#) on page 87

[Configuring DNS settings](#) on page 87

Related tasks

[Viewing network settings](#) on page 83

[Configuring hosts](#) on page 85

Adding a host name mapping

You can add a host name mapping, while adding a new host name, if necessary.

Steps

1. Select **Add** in the Hosts Mapping area to create a host mapping.
2. If no hosts are listed in the Host Name list, select the add (+) button.
3. In the Add Host dialog, enter an IP address and one or more host names that will be used for the mapping.
The new host name is added to the list of Host Names. Continue to add host names as necessary.
4. Select **Add**.
The mapping is created, and you are returned to the Hosts page.
5. To save the newly created Host Mapping, click on **Apply**.

Related tasks

[Deleting a host name mapping](#) on page 86

Deleting a host name mapping

You can delete a host name mapping through the Host Name mapping table.

Steps

1. In the **Mapping** table, select the rows you want to delete.
2. Click the **Delete** button above the Mapping table.
3. Click **Apply** to save the changes.
4. Select **Close** when the Completed message appears.
You are returned to the Settings tab.

Related tasks

[Adding a host name mapping](#) on page 86

Configuring DNS settings

DNS settings can be configured from the **Settings** page, which is accessed by clicking the gear icon in the upper right corner.

Related concepts

[Managing a domain search list](#) on page 87

[Mapping hosts](#) on page 86

Related tasks

[Viewing network settings](#) on page 83

[Configuring hosts](#) on page 85

Adding a DNS IP address

DNS servers are shown in a table with Add and Delete button options.

Steps

1. Determine the method for obtaining the DNS. Choose to either:
 - Obtain DNS Settings using DHCP. (At least one interface must be configured using DHCP.)
 - Manually configure DNS:
 - a. Select the plus (+) button.
 - b. Enter the DNS IP address.
2. Select **Apply** to save changes.

Related tasks

[Deleting a DNS IP address](#) on page 87

Deleting a DNS IP address

DNS servers are shown in a table with Add and Delete button options.

Steps

1. Select the one or more rows from the table listing.
2. Click the Delete (**X**) button on the DNS IP address in the table to be deleted.
3. Select **Apply** to save changes.

Related tasks

[Adding a DNS IP address](#) on page 87

Managing a domain search list

You can add or remove a domain from a domain search list.

Related concepts

[Mapping hosts](#) on page 86

[Configuring DNS settings](#) on page 87

Related tasks

[Viewing network settings](#) on page 83

[Configuring hosts](#) on page 85

Adding a search domain

Search Domains are shown as an Action table within the DNS page.

Steps

1. Click the **Add** button (+) next to "Search domain names".
2. Enter a name in the "Search domain" text box.
3. Select **Add**.

Results

You should be returned to the DNS page with the newly added Search Domain added to the list.

Related tasks

[Removing a search domain](#) on page 88

Removing a search domain

Search Domains are shown as an Action table within the DNS page.

Steps

1. Select the search domains to delete from the "Search domain names" list.
2. Click the **Delete** button (X) above the table.
3. Select **Apply**.

Results

Changes are applied to the system.

Related tasks

[Adding a search domain](#) on page 88

Configuring routes

Routes determine the path taken to transfer data to and from the local host (DDMC) to another network or host.

DDMC does not generate or respond to any of the network routing management protocols (RIP, EGRP/EIGRP, and BGP). The only routing implemented on DDMC is based on the internal route table, where the administrator may define a specific network or subnet used by a physical interface (or interface group).

DDMC uses *source-based routing*, which means outbound network packets that match the subnet of multiple interfaces will be routed over the physical interface from which they originated.

NOTE: The routing for connections initiated from DDMC (such as for replication) depend on the source address used for interfaces using the same subnet. To force traffic for a specific interface to a specific destination (even if that interface is on the same subnet as other interfaces), you can configure a static routing entry between two systems that will override source routing.

Related concepts

[Configuring network interfaces](#) on page 84

[Configuring network settings](#) on page 83

Viewing route information

The Routes pages provides details about all of the routing information for your DDMC setup, including the default gateway values, and static and dynamic routes.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Network > Routes**.
2. On the Routes page, view the configured static and dynamic routes (described in the following table), and create or modify routing information.

Table 17. Route information

item	description
Default IPv4 Gateway	Address of the default IPv4 gateway.
Default IPv6 Gateway	Address of the default IPv6 gateway.
Static Routes	Static routes that are either network or host-based routes.
Route Spec	Route specification being used to configure routes.
Dynamic Routes	Dynamically assigned routes that use network or host paths for data transmission.
Destination	Destination host/network where the network traffic (data) is sent.
Gateway	Address of the router in the DDMC network or 0.0.0.0 if no gateway is set.
Genmask	Netmask for the destination net. Initially set to 255.255.255.255 for a host destination and 0.0.0.0 for the default route.
Flags	Possible values include: U – Route is up. H – Target is a host. G – Use gateway. R – Reinstate route for dynamic routing. D – Dynamically installed by daemon or redirect. M – Modified from routing daemon or redirect. A – Installed by addrconf. C – Cache entry. ! – Reject route.
Metric	Distance to target (usually counted in hops). (It is not used by the DD OS, but might be needed by routing daemons.)
MTU	Maximum Transfer Unit (MTU) size for physical (Ethernet) interface.
Window	Default window size for TCP connections over this route.
IRTT	Initial RTT (Round Trip Time). The kernel uses this to estimate the best TCP protocol parameters without waiting on (possibly slow) answers.
Interface	Interface name associated with routing interface.

Related tasks

[Setting the default IPv4 or IPv6 gateway address](#) on page 90

[Creating static routes](#) on page 90

[Deleting static routes](#) on page 90

Setting the default IPv4 or IPv6 gateway address

You can set the default IPv4 or IPv6 gateway address by using the DHCP server or by manually configuring it.

Steps

1. The Default IPv4 Gateway or the Default IPv6 Gateway can be set using the DHCP value or a manually configured gateway.
 - a. **Use DHCP value:** indicates that you want to use the DHCP (Dynamic Host Configuration Protocol) server value.
 - b. **Manually Configure** Indicates that you want to manually configure the gateway address and enables the **Gateway** box, into which you should enter the gateway address. Changing the mode from DHCP to Manual will provide a text box for you to specify the default gateway.
2. Click **Apply** to save the changes.

Related tasks

[Viewing route information](#) on page 89

[Creating static routes](#) on page 90

[Deleting static routes](#) on page 90

Creating static routes

To force traffic for a specific interface to a specific destination (even if that interface is on the same subnet as other interfaces), you can configure a static routing entry between two systems that override source routing.

Steps

1. Select **Add** in the Static Routes action table to create a route.
2. In the Add Static Routes dialog box, select an interface.
3. Specify the **Destination** by selecting one of the following:
 - **Network** – Type the network IP address and netmask.
 **NOTE:** This is not the IP address of the interface.
 - **Host** – Type the hostname or IP address of the destination host of the route.
4. Optionally, type a new gateway address in the **Gateway** box.
5. Select **Add** to close the dialog box and save changes.

The new route is now added to the Static Routes table in the Routes page.
6. To save the newly created Route Spec, click **Apply**.

Related tasks

[Viewing route information](#) on page 89

[Setting the default IPv4 or IPv6 gateway address](#) on page 90

[Deleting static routes](#) on page 90

Deleting static routes

You can delete static routes when you no longer need them.

Steps

1. In the **Route Spec** area, select the route specification to delete.
2. Select **Delete**.

The Delete Route dialog box appears.
3. Select **Delete** and **Close**.

The selected route specification is removed from the Route Spec list.

4. Click **Apply** to save the changes to the routes list.

Related tasks

- [Viewing route information](#) on page 89
- [Setting the default IPv4 or IPv6 gateway address](#) on page 90
- [Creating static routes](#) on page 90

Working with SNMP

To monitor DDMC using SNMP, you will need to install the DD MIB in your SNMP Management system. The DD MIB will allow SNMP queries for DD-specific information.

DDMC also supports the standard MIB-II so you can also query MIB-II statistics for general data such as network statistics. For full coverage of available data you should use both the Data Domain MIB and the standard MIB-II MIB.

DDMC supports SNMP V2C and/or SNMP V3. SNMP V3 provides a greater degree of security than V2C by replacing cleartext community strings (as a means of authentication) with user-based authentication using either MD5 or SHA1. Also with SNMP V3, user authentication packets can be encrypted and their integrity verified with either DES or AES.

The default port that is open when SNMP is enabled is port 161. Traps are sent out through port 162.

Related tasks

- [Configuring mail server settings](#) on page 117
- [Configuring time and date settings](#) on page 116
- [Configuring system properties](#) on page 117

Checking SNMP status and configuration

The SNMP page shows SNMP status and properties, and the SNMP V3 and SNMP V2C configuration.

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Network > SNMP**.
2. View information about SNMP, as described in the following tables.

Table 18. SNMP status

Item	Description
Status	Operational status of the SNMP agent on DDMC: Enabled or Disabled.

Table 19. SNMP properties

Item	Description
SNMP System Location	Location of DDMC.
SNMP System Contact	Administrator for DDMC.

Table 20. SNMP V3 configuration

Item	Description
SNMP Users	
Name	Name of the user on the SNMP manager with access to the agent for DDMC.
Access	Access permissions for the SNMP user: <ul style="list-style-type: none">• Read-only• Read-write
Authentication Protocols	Authentication protocol for validating SNMP user: <ul style="list-style-type: none">• MD5• SHA1• None

Table 20. SNMP V3 configuration (continued)

Item	Description
Privacy Protocol	Encryption protocol for validating SNMP user: <ul style="list-style-type: none"> • AES • DES • None
Trap Hosts	
Host	IP address or domain name of the SNMP management host.
Port	Port that is used for SNMP trap communication with the host. Port 162 is the default.
User	User on trap host authenticated to access DD SNMP information.

Table 21. SNMP V2C configuration

Item	Description
Communities	
Community	Name of the community, for example, public, private, or localCommunity.
Access	Access permission that is assigned: <ul style="list-style-type: none"> • Read-only • Read-write
Hosts	The hosts in this community.
Trap Hosts	
Host	Systems that are designated to receive SNMP traps that are generated by DDMC. If this parameter is set, systems receive alert messages, even if the SNMP agent is disabled.
Port	Port that is used for SNMP trap communication with the host. Port 162 is the default.
Community	Name of the community, for example, public, private, or localCommunity.

Related concepts

[Managing SNMP V3 users](#) on page 94

[Managing SNMP V3 and V2C trap hosts](#) on page 95

[Managing SNMP V2C communities](#) on page 96

Related tasks

[Enabling or disabling SNMP](#) on page 92

[Downloading the SNMP MIB](#) on page 93

[Configuring SNMP properties](#) on page 93

Enabling or disabling SNMP

You can enable or disable SNMP through DDMC.

Steps

1. In the Status area, select **Enable** to use SNMP.
2. In the Status area, select **Disable** to stop using SNMP.
3. Click **Apply** to save changes.

Related concepts

- [Checking SNMP status and configuration](#) on page 91
- [Managing SNMP V3 users](#) on page 94
- [Managing SNMP V3 and V2C trap hosts](#) on page 95
- [Managing SNMP V2C communities](#) on page 96

Related tasks

- [Downloading the SNMP MIB](#) on page 93
- [Configuring SNMP properties](#) on page 93

Downloading the SNMP MIB

You can download the SNMP MIB through DDMC.

Steps

1. In the Status area, select **Download MIB file**.
2. In the Opening DATA_DOMAIN.mib dialog, select **Save**.

Related concepts

- [Checking SNMP status and configuration](#) on page 91
- [Managing SNMP V3 users](#) on page 94
- [Managing SNMP V3 and V2C trap hosts](#) on page 95
- [Managing SNMP V2C communities](#) on page 96

Related tasks

- [Enabling or disabling SNMP](#) on page 92
- [Configuring SNMP properties](#) on page 93

Configuring SNMP properties

You can configure SNMP system location and system contacts.

Steps

1. In the SNMP text fields, add an SNMP system location (a description of where DDMC is located) and/or an SNMP system contact (for example, the email address of the system administrator for DDMC).
2. Select **OK**.
3. Click **Apply** to save changes.

Related concepts

- [Checking SNMP status and configuration](#) on page 91
- [Managing SNMP V3 users](#) on page 94
- [Managing SNMP V3 and V2C trap hosts](#) on page 95
- [Managing SNMP V2C communities](#) on page 96

Related tasks

- [Enabling or disabling SNMP](#) on page 92
- [Downloading the SNMP MIB](#) on page 93

Managing SNMP V3 users

Procedures for managing V3 users including creating, modifying, and removing user accounts. Users on the SNMP manager have access to the agent for DDMC.

Related concepts

[Checking SNMP status and configuration](#) on page 91

[Managing SNMP V3 and V2C trap hosts](#) on page 95

[Managing SNMP V2C communities](#) on page 96

Related tasks

[Enabling or disabling SNMP](#) on page 92

[Downloading the SNMP MIB](#) on page 93

[Configuring SNMP properties](#) on page 93

Creating SNMP V3 users

You can set up SNMP V3 users using the Action table on the SNMP Settings page.

Steps

1. In the V3 Configuration Users area, select **Add**.
The **Add SNMP V3 User** dialog appears.
2. In the Name text field, enter the name of the user or the SNMP manager who will have access to the agent for DDMC. The name must be a minimum of 8 characters.
3. Select either read-only or read-write access for this user.
4. To authenticate the user, select the checkbox for **Authentication**.
 - a. Select either the MD5 or the SHA1 protocol.
 - b. Enter the authentication key in the Key text field.
 - c. To provide encryption to the authentication session, select the checkbox next to **Privacy**.
 - d. Select either the AES or the DES protocol.
 - e. Enter the encryption key in the Key text field.
5. Select **Apply**.
The newly added user account appears in the SNMP V3 Users table.

Related tasks

[Modifying SNMP V3 users](#) on page 94

[Removing SNMP V3 users](#) on page 95

Modifying SNMP V3 users

You can modify a variety of information about SNMP V3 users.

Steps

1. In the Action table under the V3 Configuration section on the SNMP Settings page, select **Edit**.
The **Edit SNMP User** dialogue.
2. Select either read-only or read-write access for this user.
3. To authenticate the user, select the checkbox for **Authentication**.
 - a. Select either the MD5 or the SHA1 protocol.
 - b. Enter the authentication key in the Key text field.
 - c. To provide encryption to the authentication session, select the checkbox next to **Privacy**.

- d. Select either the AES or the DES protocol.
 - e. Enter the encryption key in the Key text field.
4. Select **Apply**.

The new settings for this user account are displayed in the SNMP Users table.

Related tasks

[Creating SNMP V3 users](#) on page 94

[Removing SNMP V3 users](#) on page 95

Removing SNMP V3 users

If an SNMP V3 user is being used by one or more trap hosts, you must first delete the trap hosts before deleting the user.

Steps

1. In the Action table under the V3 Configuration section on the SNMP Settings page, select **Delete**.
2. Verify the user name to be deleted, and select **Apply**.

 **NOTE:** If the **Delete** button is disabled, the selected user is being used by one or more trap hosts. Delete the trap hosts, and then delete the user.

The user account is removed from the SNMP Users table.

Related tasks

[Creating SNMP V3 users](#) on page 94

[Modifying SNMP V3 users](#) on page 94

Managing SNMP V3 and V2C trap hosts

Managing SNMP V3 and V2C trap hosts includes creating, modifying, and removing hosts that received SNMP traps.

Related concepts

[Checking SNMP status and configuration](#) on page 91

[Managing SNMP V3 users](#) on page 94

[Managing SNMP V2C communities](#) on page 96

Related tasks

[Enabling or disabling SNMP](#) on page 92

[Downloading the SNMP MIB](#) on page 93

[Configuring SNMP properties](#) on page 93

Creating SNMP V3 and V2C trap hosts

You can create SNMP V3 and V2C trap hosts using the Action table on the SNMP Settings page.

Steps

1. In the SNMP V3 Trap Hosts or SNMP V2C Trap Hosts area, select **Add**.

The **Add SNMP [V3 or V2C] Trap Hosts** dialog appears.

2. In the Host text field, enter the IP address or domain name of the SNMP Host where traps will be sent.
3. In the Port text field, enter the port number for sending traps (port 162 is commonly used).
4. Select the user (SNMP V3) or the community (SNMP V2C) from the drop-down menu.

Alternately, from the drop-down menu select Create New User (SNMP V3) to add an SNMP user, or Create New Community (SNMP V2C) to add an SNMP community.

5. Select **Apply**.

Related tasks

[Modifying SNMP V3 and V2C trap hosts](#) on page 96

[Removing SNMP V3 and V2C trap hosts](#) on page 96

Modifying SNMP V3 and V2C trap hosts

You can modify the port, user, and/or community for an SNMP V3 or V2C trap host using the Action table on the SNMP Settings page..

Steps

1. In the Trap Hosts area (either for V3 or V2C), select a Trap Host entry and select **Edit**.
The **Edit SNMP [V3 or V2C] Trap Hosts** dialog appears. Modify any of the following items.
2. In the Port text field, enter the port number for sending traps (port 162 is commonly used).
3. Select the user (SNMP V3) or the community (SNMP V2C) from the drop-down menu.
4. Select **Apply**.

Related tasks

[Creating SNMP V3 and V2C trap hosts](#) on page 95

[Removing SNMP V3 and V2C trap hosts](#) on page 96

Removing SNMP V3 and V2C trap hosts

You can remove SNMP V3 and V2C trap hosts using the Action table on the SNMP Settings page..

Steps

1. In the Trap Hosts area (either for V3 or V2C), select a trap host entry, and select **Delete**.
2. Verify the host name to be deleted, and select **Apply**.

The trap host entry is removed from the Trap Hosts table.

Related tasks

[Creating SNMP V3 and V2C trap hosts](#) on page 95

[Modifying SNMP V3 and V2C trap hosts](#) on page 96

Managing SNMP V2C communities

The Community string is sent in cleartext and is very easy to intercept. If this occurs, the interceptor can retrieve information from devices on your network, modify their configuration, and possibly shut them down. Instead, using the SNMP V3 Users configuration provides authentication and encryption to avoid this.

Related concepts

[Checking SNMP status and configuration](#) on page 91

[Managing SNMP V3 users](#) on page 94

[Managing SNMP V3 and V2C trap hosts](#) on page 95

Related tasks

[Enabling or disabling SNMP](#) on page 92

[Downloading the SNMP MIB](#) on page 93
[Configuring SNMP properties](#) on page 93

Creating SNMP V2C communities

You can create SNMP V2C communities using the Action table on the SNMP Settings page.

Steps

1. In the Communities area, select **Add**.
The **Create SNMP V2C Community** dialog appears.
2. In the Community text field, enter the community name of the SNMP manager who will have access to the agent for DDMC.
The community name must be a minimum of 8 characters.
3. Select either read-only or read-write access for this community.
4. In the Hosts area, select the checkbox of a host in the list, or:
 - a. Select **+** to add a host.
The Host dialog appears.
 - b. In the Host text field, enter the IP address or domain name of the host.
 - c. Select **OK**.
The Host is added to the host list.
5. Select **Apply**.
The new community entry appears in the Communities table.

Related tasks

[Modifying SNMP V2C communities](#) on page 97
[Deleting SNMP V2C communities](#) on page 98

Modifying SNMP V2C communities

You can modify SNMP V2C communities using the Action table on the SNMP Settings page..

Steps

1. In the Communities area, select a checkbox for the community, and select **Edit**.
The **Modify SNMP V2C Community** dialog appears. Add or change any of the following settings.
2. Select either read-only or read-write access for this community.
3. In the Hosts area, select the checkbox of a new host in the list, or:
 - a. Select **+** to add a host.
The Host dialog appears.
 - b. In the Host text field, enter the IP address or domain name of the host.
 - c. Select **OK**.
The Host is added to the host list.
4. Select **Apply**.
The modified community entry appears in the Communities table.

Related tasks

[Creating SNMP V2C communities](#) on page 97
[Deleting SNMP V2C communities](#) on page 98

Deleting SNMP V2C communities

If an SNMP V2C community is being used by a trap host, you must first delete the trap host before you can delete the community.

Steps

1. In the Communities area, select a checkbox for the community, and select **Delete**.

NOTE: If the **Delete** button is disabled, the selected community is being used by one or more trap hosts. Delete the trap hosts, and then delete the community.

2. Verify the community name to be deleted, and select **Apply**.
The community entry is removed from the Communities table.

Related tasks

[Creating SNMP V2C communities](#) on page 97

[Modifying SNMP V2C communities](#) on page 97

Managing access to DD Management Center

Access management includes viewing and configuring the services that provide administrator and user access to DD Management Center.

Roles required for DDMC tasks

Since mutual trust is established between DDMC and its managed systems, if a user is added to DDMC with *admin* or *limited-admin* level access, that user can also access the managed systems by launching DD System Manager to perform admin-level operations. Also, an admin-level user or limited-admin user can upgrade a managed system. Therefore, you should give each new DDMC user the same consideration that you would a new DD System Manager user.

The roles available in DDMC are the same as those in DD System Manager:

- *admin*, the *DDMC Administrator*. An admin can access all functions on a DDMC page.
- *limited-admin*, a *DDMC Limited-Administrator*. The limited-admin role can configure and monitor the Data Domain or PowerProtect system with some limitations. Users who are assigned this role cannot perform data deletion operations, edit the registry, or enter bash or SE mode.
- *user*, a *DDMC User*. A user, which can be a stand-alone user or part of a group, has access to only certain functions on a DDMC page, based on the role assigned to that user or group.

The following table shows the actions available for each feature of DDMC. [This table is provided to show when only the *user* role is required. The *admin* role can perform all tasks, as previously mentioned.]

Table 22. DDMC Roles required for DDMC tasks

Action	Minimum permission	Description of actions
Manage permissions	<ul style="list-style-type: none">• Administrator• Limited-Administrator	Assign, edit, remove permissions for users. It should be noted that the DDMC Administrator role or its associated system cannot be deleted in the permission page.
Manage Data Domain systems	<ul style="list-style-type: none">• Administrator• Limited-Administrator	Add, edit, delete systems from the inventory
Manage users/user groups	<ul style="list-style-type: none">• Administrator• Limited-Administrator	Add, edit, and delete local users; Administrator can also add, edit, and delete AD/NIS and LDAP user groups. Only the Administrator User can add, edit, and delete another user with the same role.
Configure DDMC	<ul style="list-style-type: none">• Administrator	Work with DDMC Settings pages

Table 22. DDMC Roles required for DDMC tasks (continued)

Action	Minimum permission	Description of actions
	<ul style="list-style-type: none"> Limited-Administrator 	
Upgrade systems	On the system to upgrade: <ul style="list-style-type: none"> Administrator Limited-Administrator User 	Run the System Upgrade function
Upgrade DDMC	<ul style="list-style-type: none"> Administrator Limited-Administrator 	Run the DDMC Upgrade function
Manage groups	<ul style="list-style-type: none"> Administrator Limited-Administrator 	Create, edit, delete groups
Manage properties	<ul style="list-style-type: none"> Administrator Limited-Administrator 	Create, edit, delete properties
Assign properties	<ul style="list-style-type: none"> Administrator Limited-Administrator 	Assign properties to systems
Assign to groups	<ul style="list-style-type: none"> Administrator 	Assign systems to groups
Manage reports	<ul style="list-style-type: none"> Administrator Limited-Administrator 	Create report templates and schedule report creation
Manage dashboard widgets	<ul style="list-style-type: none"> Administrator Limited-Administrator 	Create dashboard widgets
Configure dashboard	<ul style="list-style-type: none"> Administrator Limited-Administrator 	Configure widgets and dashboard layouts
Manage global filter rules	<ul style="list-style-type: none"> User 	Add, edit, delete filter rules
Launch DD System Manager	<ul style="list-style-type: none"> User 	Launch the virtual DD System Manager  NOTE: Administrator privilege is required on the managed system to change anything.
Manage user jobs	<ul style="list-style-type: none"> User 	Suspend, resume, cancel jobs owned by user
Manage all jobs	<ul style="list-style-type: none"> Administrator 	Suspend, resume, cancel any job
Manage advanced replication	<ul style="list-style-type: none"> Administrator Limited-Administrator 	View replication status, export to CVS file, assign properties
Manage basic replication	<ul style="list-style-type: none"> User 	View replication status, export to CVS file

Related concepts

[Managing local user access to DDMC](#) on page 103

Managing administrator access

Administrator Access provides settings to configure how users can connect to DDMC. Each protocol is configured separately, using the procedures in this section.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Administrator Access**.
2. View the **Passphrase**, if it is set, or set it, if not. The Passphrase is a human-readable (understandable) key – like a smart card – which is used to generate a machine-usable AES 256 encryption key. (For more information, see the *DD OS Administration Guide*.) You can also view the available services, and for a selected service, the service options that are configured for it.

Table 23. Details

Item	Description
Name	Name of a service/protocol that can access the system. One of the following protocols can be selected (for viewing or configuring): FTP, FTPS, HTTP/HTTPS, SCP/SSH, or Telnet.
Enabled	Status of the service: either enabled or disabled.
Allowed Hosts	Access permissions set for the named host.

Table 24. Protocol options

Protocol name	Option name	Description
FTP	Session Timeout	Configured number of elapsed seconds before the service times out, or Infinite.
FTPS	Session Timeout	Configured number of elapsed seconds before the service times out, or Infinite.
HTTP/HTTPS	HTTP/HTTPS port	If applicable, port number opened for the HTTP/HTTPS protocol (HTTP – port 80, by default; HTTPS – port 443, by default).
	Session Timeout	Configured number of elapsed seconds before the service times out, or Infinite.
SCP/SSH	SCP/SSH port	If applicable, port number opened for the SCP/SSH protocol (port 22, by default).
	Session Timeout	Configured number of elapsed seconds before the service times out, or Infinite.
Telnet	Session Timeout	Configured number of elapsed seconds before the service times out, or Infinite.

Managing FTP access

You can provide access to DDMC through an FTP connection.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Administrator Access**.
2. In the **Services** area, select FTP, and click **Edit**.
3. In the Access dialog, select **Enabled** or **Disabled**. If FTPS is enabled, it will be disabled before enabling FTP.
4. In **Session Timeout**, enter, in seconds, the interval that must elapse before the connection closes, or choose the default of **Infinite**.

5. Determine how hosts are to connect:
 - **All hosts**
 - **Specified hosts** – Host names can be a fully qualified host name or an IP address.
 - To add a host, select Add (green plus sign). Enter the host name, and click **Save**.
 - To modify a host name, select the host name in the **Hosts** list, click Edit (pencil), change the host name, and click **Save**.
 - To remove a host name, select the host name in the **Hosts** list, click Delete (X), and click **Save**.
6. Click **Apply** to save changes.

Managing FTPS access

You can provide access to DDMC through an FTPS connection.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Administrator Access**.
2. In the **Services** area, select FTPS, and click **Edit**.
3. In the Access dialog box, select **Enabled** or **Disabled**. If FTP is enabled, it is disabled before enabling FTPS.
4. In **Session Timeout**, type, in seconds, the interval that must elapse before the connection closes, or choose the default of **Infinite**. To return to default values, select the **Default** button.
5. Determine how hosts are to connect:
 - **All hosts**
 - **Specified hosts** – Host names can be a fully qualified hostname or an IP address.
 - To add a host, select Add (green plus sign). Type the hostname, and click **Save**.
 - To modify a hostname, select the hostname in the **Hosts** list, click Edit (pencil), change the hostname, and click **Save**.
 - To remove a hostname, select the hostname in the **Hosts** list, click Delete (X).
6. Click **Apply** to save changes.

Managing HTTP/HTTPS access

You can provide access to DDMC through an HTTP and/or HTTPS connection.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Administrator Access**.
2. In the **Services** area, select **HTTP/HTTPS**, and click **Edit**.
3. In the Edit HTTP/HTTPS Access dialog box, select **Enabled** or **Disabled**, and a port for HTTP and HTTPS.
4. In **Session Timeout**, type, in seconds, the interval that must elapse before the connection closes, or choose **Infinite**. The default value is 10,800 seconds (3 hours).
5. Determine how hosts are to connect:
 - **All hosts**
 - **Specified hosts** – Host names can be a fully qualified hostname or an IP address.
 - To add a host, select Add (green plus sign). Type the hostname, and click **Save**.
 - To modify a hostname, select the hostname in the **Hosts** list, click Edit (pencil), change the hostname, and click **Save**.
 - To remove a hostname, select the hostname in the **Hosts** list, click Delete (X), and click **Save**.
6. Click **Apply** to save changes.

Results

Table 25. HTTP/HTTPS enabled or disabled

HTTP enabled	HTTPS enabled	Navigate to DDMC using HTTP
X		Uses HTTP
	X	Shows server down page
		Shows server down page
X	X	Redirects to HTTPS

Managing SCP/SSH access

You can provide access to DDMC through an SCP and/or SSH connection.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Administrator Access**.
2. In the **Services** area, select **SSH/SCP**, and click **Edit**.
3. In the Edit HTTP/HTTPS Access dialog box, select **Enabled** or **Disabled**, and a port for SSH and SCP.
4. In **Session Timeout**, type, in seconds, the interval that must elapse before the connection closes, or choose the default value of **Infinite**.
5. Determine how hosts are to connect:
 - **All hosts**
 - **Specified hosts** – Host names can be a fully qualified hostname or an IP address.
 - To add a host, select Add (green plus sign). Type the hostname, and click **Save**.
 - To modify a hostname, select the hostname in the **Hosts** list, click Edit (pencil), change the hostname, and click **Save**.
 - To remove a hostname, select the hostname in the **Hosts** list, click Delete (X), and click **Save**.
6. Click **Apply** to save changes.

Managing Telnet access

You can provide access to DDMC through a Telnet connection.

About this task

 **NOTE:** Due to FIPS compliance, Telnet can be uninstalled in DDMC through the CLI. If it is uninstalled, Telnet will not be part of the protocol list in DDMC.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Administrator Access**.
2. In the **Services** area, select Telnet, and click **Edit**.
3. In the Access dialog box, select **Enabled** or **Disabled**.
4. In **Session Timeout**, type, in seconds, the interval that must elapse before the connection closes, or choose the default of **Infinite**. To return to default values, select the **Default** button.
5. Determine how hosts are to connect:
 - **All hosts**
 - **Specified hosts** – Host names can be a fully qualified hostname or an IP address.
 - To add a host, select Add (green plus sign). Type the hostname, and click **Save**.
 - To modify a hostname, select the hostname in the **Hosts** list, click Edit (pencil), change the hostname, and click **Save**.
 - To remove a hostname, select the hostname in the **Hosts** list, click Delete (X), and click **Save**.

6. Click **Apply** to save changes.

Managing certificates

About this task

Certificates are managed by importing CA root and CA intermediate files through the GUI.

CA files provide the following:

- Allows only https application for imported host type.
- Imported host type allows file type to import a PKCS 12 file (. p12), a signed public file (. pem) or use certificate text.
- Can upload a PKCS 12 file (.p12) or a signed public file (. pem) for imported host type.
- Imported p12 file require password.
- User has the option to generate a certificate signing request when select . pem file type option for imported host type.
- User can paste certificate content into the certificate text area as import certificate.

CA intermediate files provide the following:

- Allows only trusted CA application for imported CA type.
- Imported CA type allows file type to import a signed public file (. pem) or use certificate text.

Steps

1. To import CA Root, enter the following command in Windows or Linux CLI:

```
ssh sysadmin@DDMC adminaccess certificate import ca application  
login-auth < rootCA.crt
```

2. To import the intermediate CA files, enter the following command in the CLI:

```
ssh sysadmin@DDMC adminaccess certificate import ca application  
login-auth < intermediateCA.crt
```

Managing local user access to DDMC

The extent to which you can manage local user access to DDMC depends on your role.

If you are an *administrator* on DDMC, you become a *global administrator*, and you can configure and monitor all managed Data Domain and PowerProtect systems.

If you are a *user* on DDMC, you can view only the managed Data Domain and PowerProtect systems to which you have been assigned a *user*, *admin*, or *limited-admin* role by a DDMC administrator.

Related concepts

[Roles required for DDMC tasks](#) on page 98

Related tasks

[Logging into DDMC](#) on page 26

Viewing local user information

The timestamps in the user-authentication module use Greenwich Mean Time (GMT). Therefore, when configuring expiration dates for disabling a user's account and password, the expiration date should reflect GMT instead of local time.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Local Users**.
2. On the Local Users page, view information for the configured users.

Table 26. Information for configured users

Item	Description
Name	User ID, as added to the system.
Role	<p>Possible roles of users based on a set of privileges:</p> <ul style="list-style-type: none"> • <i>admin role</i>: Can configure and monitor the entire system. • <i>limited-admin role</i>: Can configure and monitor the entire system, but cannot delete/destroy Mtree data. • <i>user role</i>: Can monitor systems and perform the fastcopy operation. <p>Users with admin roles can view all users. Users with user roles can view only their own user account.</p>
Status	<ul style="list-style-type: none"> • enabled – User access to the account is permitted. • disabled – User access to the account is denied because the expiration date for the account has been reached or a locked account’s password has not been renewed. Admin users can disable/enable users with admin, limited-admin, or user roles, except SysAdmin User. No users can disable SysAdmin. Security officers can disable/enable only other security officers. • locked – User access to the account is denied because the password has expired.
Disable Date	Date the account is set to be disabled.
Last Login From	Location where the user last logged in.
Last Login Time	Time the user last logged in.

3. Select a specific user to see Detailed Information.

Table 27. Specific user detailed information

Item	Description
Password Last Changed	Date the password was last changed.
Minimum Days Between Change	Minimum number of days between password changes that you allow a user. Default is 0.
Maximum Days Between Change	Maximum number of days between password changes that you allow a user. Default is 90.
Warn Days Before Expire	Number of days to warn the users before their password expires. Default is 7.
Disable Days After Expire	Number of days after a password expires to disable the user account. Default is never.

 **NOTE:** The default password policy can be changed by an admin or limited-admin by selecting **Manage Password Policies**. Default values are the initial default password policy values.

Related concepts

[User roles](#) on page 105

Related tasks

[Creating local users](#) on page 105

[Modifying a local user profile](#) on page 106

[Deleting a local user](#) on page 107

[Enabling or disabling local users](#) on page 107

[Changing user passwords](#) on page 108

[Changing login options](#) on page 108

User roles

Roles provide a way to restrict user access to system functions by using a set of privileges. Permissions allow an admin or limited-admin access to specific groups and systems, reducing the need to configure every user as a global admin.

DDMC supports the following roles:

- *admin role*: This role can configure and monitor the entire DDMC system.
NOTE: It is recommended that the admin role be used judiciously and assigned to very few users, as these users will be able to configure DDMC as well as have access to all registered systems.
- *limited-admin role*: This role can configure and monitor the entire DDMC system, but it cannot delete or destroy MTrees.
- *user role*: This role can monitor DDMC and systems for which the user has permission.

Related tasks

[Viewing local user information](#) on page 103

[Creating local users](#) on page 105

[Modifying a local user profile](#) on page 106

[Deleting a local user](#) on page 107

[Enabling or disabling local users](#) on page 107

[Changing user passwords](#) on page 108

[Changing login options](#) on page 108

Creating local users

You can create users with either the *admin*, *limited-admin*, or the *user* role.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Local Users**.
2. Click **Add**.
3. In the Add local User dialog box, type the following in the General tab:

Table 28. General tab

Item	Description
Name	User ID or name.
Role	Management role assigned to the user: <ul style="list-style-type: none">• <i>Administrator</i> and <i>limited-admin</i>: Can configure and monitor the entire DDMC and all Data Domain systems.• <i>User</i>: Can monitor DDMC and systems for which they have permission.
Password	User password. Set a default password, and the user can change it later. The default value for the minimum length of a password or minimum number of character classes required for a user password is 1. Allowable character classes include: <ul style="list-style-type: none">• lowercase letters (a-z)• uppercase letters (A-Z)• numbers (0-9)• special characters (\$, %, #, +, and so on)
Verify Password	User password, again.
Disable account on the following date	Select Manual and type a date (mm/dd/yyyy) when you want to disable this account, or use the default value of never. This date uses GMT.
Minimum Days Between Change	Minimum number of days between password changes that you allow a user. Default is 0.
Maximum Days Between Change	Maximum number of days between password changes that you allow a user. Default is 99,999.
Warn Days Before Expire	Number of days to warn the users before their password expires. Default is 7.

Table 28. General tab (continued)

Item	Description
Disable Days After Expire	Number of days after a password expires to disable the user account. Default is Never.

4. Select **Add**.

 **NOTE:** The default password policy can be changed by the admin or limited-admin using **Manage Password Policies**. The default values are the initial default password policy values.

5. Click **Apply** to save changes.

Related concepts

[User roles](#) on page 105

Related tasks

[Viewing local user information](#) on page 103

[Modifying a local user profile](#) on page 106

[Deleting a local user](#) on page 107

[Enabling or disabling local users](#) on page 107

[Changing user passwords](#) on page 108

[Changing login options](#) on page 108

Modifying a local user profile

You can modify several aspects of a local user profile.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Local Users**.
2. Select a user name, and click **Edit**.
3. In the Edit Local User dialog: change the assigned role.
 - a. Enable or disable the user.
 - b. Change the user role.
 - c. Change the password for the user.
 - d. Set a date to disable the username.
4. Optionally change the password aging policy for the user

Table 29. Password aging policy

item	description
Minimum Days Between Change	Minimum number of days between password changes that you allow a user. Default is 0.
Maximum Days Between Change	Maximum number of days between password changes that you allow a user. Default is 99999.
Warn Days Before Expire	Number of days to warn the users before their password expires. Default is 7.
Disable Days After Expire	Number of days after a password expires to disable the user account. Default is Never.

5. Click **Save**.

Related concepts

[User roles](#) on page 105

Related tasks

[Viewing local user information](#) on page 103

[Creating local users](#) on page 105

[Deleting a local user](#) on page 107

[Enabling or disabling local users](#) on page 107

[Changing user passwords](#) on page 108

[Changing login options](#) on page 108

Deleting a local user

You can delete certain users, based on your user role. If one of the selected users cannot be deleted, the **Delete** button will be disabled. For example, sysadmin cannot be deleted.

Steps

1. From the Local Users tab, select one or more user names from the list.
2. Select **Delete** to delete the user accounts.
3. In the Delete User dialog, click **Apply** to save changes.

Related concepts

[User roles](#) on page 105

Related tasks

[Viewing local user information](#) on page 103

[Creating local users](#) on page 105

[Modifying a local user profile](#) on page 106

[Enabling or disabling local users](#) on page 107

[Changing user passwords](#) on page 108

[Changing login options](#) on page 108

Enabling or disabling local users

You can enable or disable local users.

Steps

1. From the Local Users tab, select one or more user names from the list.
2. Select either the **Enable** or **Disable** button.
3. In the Enable User or Disable User dialog, click **Apply** to save changes.

Related concepts

[User roles](#) on page 105

Related tasks

[Viewing local user information](#) on page 103

[Creating local users](#) on page 105

[Modifying a local user profile](#) on page 106

[Deleting a local user](#) on page 107

[Changing user passwords](#) on page 108

[Changing login options](#) on page 108

Changing user passwords

The Change Password dialog lets you change the password for a selected user.

Steps

1. From the Local Users tab, select a user name from the list.
2. Select **Change Password**.
3. In the Change Password dialog, enter the new password into the New Password box. (If prompted, enter the old password, as well.)
4. Enter the new password again in the Verify New Password box.
5. Click **Apply** to save changes.

Related concepts

[User roles](#) on page 105

Related tasks

[Viewing local user information](#) on page 103

[Creating local users](#) on page 105

[Modifying a local user profile](#) on page 106

[Deleting a local user](#) on page 107

[Enabling or disabling local users](#) on page 107

[Changing login options](#) on page 108

Changing login options

You can modify settings for password composition, time to change passwords, limiting login tries, and so forth.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Local Users > Manage Password Policies**.
2. In the Manage Password Policies dialog box, type the password policy information.

Table 30. Password policies

Item	Description
Minimum Days Between Change	Minimum number of days between password changes, which must be less than the (Maximum Days Between Change minus the Warn Days Before Expire). Default is 0.
Maximum Days Between Change	Maximum number of days between password changes. Default is 90.
Warn Days Before Expire	Number of days to warn a user before their password expires, which must be less than (Maximum Days Between Change minus Minimum Days Between Change). Default is 7.
Disable Days After Expire	Number of days after a password expires to disable a user account. You may type never or a number > or equal to 0. Default is never.
Minimum Length of Password	Minimum password length required. Default is 6.
Minimum Number of Character Classes	Minimum number of character classes required. Default is 1. Character classes include: <ul style="list-style-type: none">• lowercase letters (a-z)• uppercase letters (A-Z)• numbers (0-9)• special characters (\$, %, #, +, and so on)
Lowercase Character Requirement	Enable or disable the requirement for a least one lowercase character. Default is disabled.

Table 30. Password policies (continued)

Item	Description
Uppercase Character Requirement	Enable or disable the requirement for a least one uppercase character. Default is disabled.
Minimum numeric character	Enable or disable the requirement for a least one numeric character. Default is disabled.
Minimum special character	Enable or disable the requirement for a least one special character. Default is disabled.
Max Consecutive Character Requirement	Enable or disable the requirement for a maximum of three repeated characters. Default is disabled.
Enforce password reuse history	Specify the number of remembered passwords. The range is 0 to 24. Default is 1.
Maximum login tries	Specify the maximum number of login tries before a mandatory lock is applied to a user account. This limit applies to all user accounts, including sysadmin. A locked user cannot log in while the account is locked. The range is 4 to 20. Default is 4.
Unlock timeout (seconds)	Specify how long a user account is locked after the maximum number of login tries. When the configured unlock timeout is reached, a user can re-attempt to login. The range is 120 seconds to 3,600 seconds. Default is 120 seconds.

3. Click **Apply** to save changes.

Related concepts

[User roles](#) on page 105

Related tasks

[Viewing local user information](#) on page 103

[Creating local users](#) on page 105

[Modifying a local user profile](#) on page 106

[Deleting a local user](#) on page 107

[Enabling or disabling local users](#) on page 107

[Changing user passwords](#) on page 108

Active users

Active users are users that are currently logged into DDMC.

Viewing active users

You can view a variety of information about users who are currently logged in to DDMC.

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Active Users**.
2. View the list of active users displayed.

Table 31. Active users

item	description
Name	Name of user with an active session
Idle	Amount of time since last activity for user
Last Login From	System where user is logged in
Last Login Time	Datestamp when user logged in
Tty	Terminal notation for CLI login or <i>GUI</i> if user is logged in using the GUI

Configuring authentication

DDMC lets you configure three types of authentication: Active Directory, Workgroup, and NIS.

NIS authentication

Local user accounts on a Data Domain or PowerProtect system start with a UID of 500. When you set up a in an NIS (network information service) environment, be aware of potential UID conflicts between local and NIS user accounts. To avoid such conflicts, during initial planning consider the size of potential local accounts when you define allowable UID ranges for NIS users.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Authentication**.
2. Click the **NIS** tab.
3. In the NIS Authentication area, view information about NIS Servers and configured NIS Groups, as described in the following table.

Table 32. NIS Authentication Information

item	description
NIS Status	Status of service: enabled or disabled
Domain Name	Name of domain for this service
Server	Name of server performing authentication
NIS Group	Name of NIS group
Management Role	Management role assigned to group (admin or user)

4. You may add, edit, or delete any of this information by selecting the appropriate control.

Enabling NIS authentication

The NIS (network information service) domain maintains a centralized repository of users, groups, and server names. NIS adds a global directory that authenticates users from any host on the network.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Authentication**.
2. Click the **NIS** tab.
3. In the **Status** area, select **Enabled**.
4. Select **Apply**.

Disabling NIS authentication

After you have enabled NIS authentication, you may occasionally need to disable it.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Authentication**.
2. Click the **NIS** tab.
3. In the **Status** area, select **Disabled**.
4. Select **Apply**.

Configuring NIS domain names

If an NIS domain name is invalid, it may take a long time to process. Be sure to enter a valid domain name.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Authentication**.
2. Click the **NIS** tab.
3. Enter the new domain name in the Domain Name text box.
4. Click **Apply**.

Configuring NIS servers

You can manually configure NIS servers, or you can obtain them from DHCP (dynamic host configuration protocol). When you manually configure them, you can add, modify, or delete servers.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Authentication**.
2. Click the **NIS** tab.
3. In the NIS Servers area, select **Manual**.
4. To add a server, click Add (green plus sign) and specify a name.
5. To delete a server, select the server, then click Delete (red X).
6. Select **Apply**.

Configuring NIS groups

You can add, modify, or delete NIS groups.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Authentication**.
2. Click the **NIS** tab.
3. To add a group, click Add (green plus sign). Enter a name, select a management role (admin, limited-admin, or user), and click **Add**.
4. To modify a group, select the group and click Modify (pencil). Edit the name and/or management role (admin or user), and click **Save**.
5. To delete a group, select the group, and click Delete (X).
6. Click **Apply**.

Windows authentication

Windows authentication can be configured using workgroups or Active Directory.

1. Click the Settings button (the gear icon in the upper right corner) in the DDMC banner, then select **Access > Authentication**.
2. Click the **Windows** tab.
3. Select **Using Workgroup** or **Using Active Directory** from the **Method** drop-down list.

For workgroup authentication, view information about CIFS servers and configured workgroups, as described in the following table.

Table 33. CIFS servers and configured workgroup information

Item	Description
Workgroup name	Name of the workgroup the DDMC instance resides in.
CIFS server	Name of the CIFS server where the DDMC is connected.

For Active Directory authentication, view information about Active Directory, as described in the following table.

Table 34. Active Directory information

Item	Description
Realm name	Name of the Active Directory Realm.
User name	Name of the Active Directory user.
Password	Active Directory password.
CIFS server	Name of the CIFS server where the DDMC is connected.
Domain controller	Active Directory domain controller where the DDMC is connected.
Organizational unit	Name of the organizational unit the DDMC instance resides in.
Windows group	Name of the Windows group the DDMC instance resides in.

Configuring Workgroup authentication

Workgroup mode joins DDMC to a workgroup domain.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Authentication**.
2. Click the **Windows** tab.
3. Select **Using Workgroup**.
4. For Workgroup Name, select *Manual* to enter a different Workgroup name in the text box.
5. For CIFS Server Name, select *Manual* to enter a different CIFS server name (Data Domain or PowerProtect system) in the text box.
6. Click **Apply**.

Active directory authentication

If Active Directory is configured, you can use the Active Directory Authentication panel to view associated information.

Steps

Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Authentication**.

 **NOTE:** Username and password are always required to apply changes.

Configuring Active Directory authentication

DDMC must meet all Active Directory requirements, such as a clock time that differs no more than five minutes from that of the domain controller.

Steps

Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Authentication**.

Entering Realm Name and credentials

A Windows KDC (Key Distribution Center) requires the Realm Name and credentials for Active Directory authentication.

Steps

1. In the Realm Name text box, enter the complete realm name for DDMC, such as **domain1.local**.

2. In the User Name text box, enter a user name. This user could be either in a domain to be joined or in a domain that is a trusted domain of your company. This user must have permission to create accounts in this domain. The user name must be compatible with Microsoft requirements for the Active Directory domain being joined.
3. In the Password text box, enter a password. The password must be compatible with Microsoft requirements for the Active Directory domain being joined.

Configuring advanced active directory settings

You may optionally configure advanced active directory settings for CIFS Server Name, Domain Controllers, and Organizational Unit.

Steps

1. For CIFS Server Name:
 - Select *Use default: xxx* to use the default CIFS server name, or
 - Select *Manual*, and enter the CIFS server name in the text box.
2. For Domain Controllers:
 - Select *Automatically assign*, which is the default and recommended method, or
 - Select *Manual*, and enter controller name(s) in the text box(es). Up to three controller names can be added. You can enter fully qualified domain names, host names, or IP (IPv4 or IPv6) addresses.
3. For Organizational Units:
 - Select *Use default: xxx* to use the default Organization Units, or
 - Select *Manual*, and enter the Organizational Unit name in the text box.

 **NOTE:** The account is moved to the new Organizational Unit.

4. Select **OK**.

Next steps

After configuring Windows authentication, you must enable CIFS authentication from the DDMC command line:

```
adminaccess authentication add cifs
```

Creating Windows groups

A *Windows group* is a group (based on one of the user roles – admin or user) that exists on a Windows domain controller.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Authentication**.
2. Click the **Windows** tab.
3. Select **Using Active Directory**.
4. Click **Add**.
5. Specify a windows group.
6. Specify a role.
7. Click **Add**.
8. Click **Apply**.

Modifying Windows groups

After you have created a Windows group, you can modify it, as needed.

Steps

1. Select **Administration > Settings > Access tab > Authentication**.
2. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Authentication**.
3. Click the **Windows** tab.

4. Select **Using Active Directory**.
5. Select a Windows group, and click **Edit**.
6. Edit the group name in the text box. The domain for the group must be specified, for example, domain\group name.
7. Click **Save**.
8. Click **Apply**.

Deleting Windows groups

You cannot delete default Windows groups, such as Domain Admins. If a default Windows group is selected, the Delete button will be grayed out.

Steps

1. Select **Administration > Settings > Access tab > Authentication**.
2. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Authentication**.
3. Click the **Windows** tab.
4. Select **Using Active Directory**.
5. Select a Windows group, and click **Delete**.
6. Click **Apply**.

LDAP authentication

Lightweight Directory Access Protocol (LDAP) can be used to authenticate users with DDMC access. An LDAP user can manage Data Domain systems.

About this task

 **NOTE:** Enabling LDAP status disables NIS status if NIS is enabled. Enabling NIS status disables LDAP status if LDAP is enabled.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Authentication**.
2. Click the **LDAP** tab.
3. In the LDAP Authentication area, view information about LDAP servers and configured LDAP groups, as described in the following table.

Table 35. LDAP authentication information

Item	Description
Status	Status of service: enabled or disabled
Base suffix	Point from where a server searches for users
Bind DN	Location of the user in LDAP directory tree
Bind password	Password to access bind DN
SSL	Status: enabled or disabled  NOTE: If SSL is disabled, Protocols and Demand server certificate cannot be edited.
Protocols	SSL protocol: LDAPS or StartTLS
Demand server certificate	Status: enabled or disabled
LDAP server	Name of server performing authentication
LDAP group	Name of LDAP group
Role	Management role that is assigned to group (admin or user)

4. Add, edit, or delete any of this information by selecting the appropriate control.

Enabling LDAP authentication

The LDAP (Lightweight Directory Access Protocol) server

About this task

 **NOTE:** Enabling LDAP status will disable NIS status if NIS status is enabled, and enabling NIS status will disable LDAP status if LDAP status is enabled.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Authentication**.
2. Click the **LDAP** tab.
3. In the **Status** area, select **Enabled**.
4. Select **Apply**.

Disabling LDAP authentication

After LDAP authentication is enabled, there may occasionally be instances where it needs to be disabled.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Authentication**.
2. Click the **NIS** tab.
3. In the **Status** area, select **Disabled**.
4. Select **Apply**.

Configuring LDAP base suffix

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Authentication**.
2. Click the **LDAP** tab.
3. Type the Base suffix in the text box.
4. Click **Apply**.

Configuring LDAP Bind DN

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Authentication**.
2. Click the **LDAP** tab.
3. Type the Bind DN in the text box.
4. Click **Apply**.

Configuring LDAP server

You can manually configure LDAP servers, or you can obtain them from DHCP (dynamic host configuration protocol). When you manually configure them, you can add, modify, or delete servers.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Authentication**.

2. Click the **LDAP** tab.
3. To add a server, click **Add** (green plus sign), and specify a name.
4. To delete a server, select the server, then click **Delete** (red X).
5. Select **Apply**.

Configuring LDAP groups

Add, modify, or delete LDAP groups.

About this task

- An LDAP group displays in the edit permission page user list.
- An LDAP user in a configured LDAP group can access DDMC like NIS or an AD user.
- An LDAP user who is associated with a configured LDAP group can launch DD System Manager.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **Access > Authentication**.
2. Click the **LDAP** tab.
3. To add a group, click **Add** (green plus sign). Enter a name, select a management role (admin, limited-admin, or user), and click **Add**.
4. To modify a group, select the group, and click **Edit** (pencil). Edit the name and/or management role (admin, limited-admin, or user), and click **Save**.
5. To delete a group, select the group, and click **Delete** (X).
6. Click **Apply**.

Managing general configuration settings

By accessing the Settings via the gear icon in the DDMC Banner, you can manage settings for your mail server, how time and date are obtained, and some system properties (location and default administrator's email and host name).

Configuring time and date settings

You can set or change the settings for your time zone, as well as how the timing for your system is synchronized [not synchronized or with NTP (Network Time Protocol)].

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **System > Time and Date**.
2. Set how time is synchronized:
 - To manually set the time and date, select **Manual**, type the date in the text box, and use the drop-down lists to set the time.
 - To use NTP to synchronize the time, select **NTP**, and choose how to access the NTP server:
 - **Obtain NTP Servers using DHCP** – DHCP (Dynamic Host Configuration Protocol) will automatically select a server.
 - **Manually Configure** – Add the IP address of the server in the **NTP Servers** area.
3. Select **Apply**.

 **NOTE:** Changes to the **Time and Date** settings require a DDMC restart to take full effect.

Related concepts

[Working with SNMP](#) on page 91

Related tasks

[Configuring mail server settings](#) on page 117

[Configuring system properties](#) on page 117

Configuring system properties

You can provide an admin email address to be added to the alert and autosupport notification lists, and an admin host to be added to the FTP and Telnet access lists, using the Properties configuration page in the Settings Lightbox.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **System > Properties**.
2. The Location text field shows where the system is located. [This text field is not used by DDMC (or DD OS); it is here simply for your information.]
3. In the Default Administrator section, enter an email address to be automatically added to the alert and autosupport notification lists, and a host to be automatically added to the FTP and Telnet access lists. Entering ALL in this field allows all hosts to FTP and Telnet in.
4. Click **Apply**.

Related concepts

[Working with SNMP](#) on page 91

Related tasks

[Configuring mail server settings](#) on page 117

[Configuring time and date settings](#) on page 116

Configuring mail server settings

You can set or change the name of your mail server using the Set Mail Server dialog.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **System > Properties**.
2. Enter the name of the mail server in the text box. .
3. Click **Apply**.

Related concepts

[Working with SNMP](#) on page 91

Related tasks

[Configuring time and date settings](#) on page 116

[Configuring system properties](#) on page 117

Checking a DDMC serial number

Each DDMC virtual machine has a unique serial number, which is used to identify the system in autosupport messages.

 **NOTE:** Serial numbers cannot be added or changed. They are automatically assigned.

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **System > Properties**.
2. View the serial number listed.

 **NOTE:** DDMC does not require a license, but the managed Data Domain and PowerProtect systems must have licenses for their core and optional features.

Managing alerts

You can configure settings to determine who will receive DDMC alert notifications and daily alert summaries.

DDMC and DD OS use the same alert system. Detailed information about the alert system is described in the *DD OS Administration Guide*.

Managing alert notifications

The groups that are configured to receive DDMC alert notifications are listed in the **Settings > System > Support > Notifications** tab. Selecting a group in the table populates the Details panels for alert class attributes and subscribers who receive notification when alerts reach the severity that is configured for the alert class.

Filtering the notifications list

To filter (or search for an item) in the notifications group list, type a group name and/or subscriber email in the appropriate text box in the Filter By area. Then select **Update**. The result is displayed at the top of the notification list. Select **Reset** to return the group list to the default order.

Creating a notification group

By default, all alerts are sent to the autosupport-alert@autosupport.datadomain.com email group, but additional groups can be created to receive specific classes of alert notifications.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **System > Support > Notifications**.
2. In the Real Time Alerts area, click **Add**.
3. In the Add Notification Group dialog, type a name for the group in the Group Name text box.
4. Select the alert class attributes, and set the severity level at which notifications are to be sent.
For example, you could create a CriticalWarnings group, select all classes, and set the severity level to Critical.
5. In the Subscribers panel, click Add (green plus sign), add the email address of a subscriber, and select **OK**.
6. Repeat this step for each subscriber who needs to be added to the group, and click **Add**.

Verifying subscriber emails in a notification group

You can send a test email to subscribers in a notification group to verify that the email addresses are operational.

Steps

1. In the **More Tasks** menu, select **Send Test Alert**.
2. In the Notification Groups panel, select the rows of the groups to receive the test email, then select **Next**.
3. In the Additional Email Addresses panel, add or modify email addresses, if necessary.
4. Select **Send Now**.

Modifying a notification group

You can modify several aspects of a notification group.

Steps

1. Click on the row of the group in the Notifications group table, and select **Modify**.
2. In the Modify Group dialog, select **Group Properties**, and in the Class Attributes area, add or remove classes, change any severity levels, and select **Next**.
3. The Subscribers area displays. Add or remove any subscriber email addresses, as needed, and select **Finish**.

Deleting a notification group

You can delete any notification group, except the Default notification group.

Steps

1. Select one or more rows of groups in the Notifications group table, and select **Delete**.
2. In the Delete Group dialog, verify the deletion, and select **OK**.
3. Select **OK** to exit the confirmation dialog.

Resetting a notification group

You can remove all notification groups that were added and remove any changes to the Default group.

Steps

1. From the **More Tasks** menu, select **Reset Notification Groups**.
2. In the Reset Notification Groups dialog, select **Yes**, and in the Verification dialog, select **OK**.

Managing a subscriber list

You can add, modify, or delete email addresses from a notification group subscriber list.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **System > Support > Notifications**.
2. Select the desired notification group, and click **Edit**.
3. In the Edit Subscribers dialog, select one of the following options:
 - To add a subscriber, click Add (green plus sign). Enter the email address in the Email Address dialog, and click **Add**.
 - To modify an email address, select the email address in the Subscriber Email list, and click Modify (pencil). Edit the email address in the Email Address dialog, and click **Save**.
 - To delete an email address, select the email address in the Subscriber Email list, and click Delete (X).
4. Click **Apply**.

Managing daily alert summaries

Every morning at 8:00 a.m. local time for the DD Management Center, a Daily Alert Summary email, which contains summaries of alerts and log messages, is sent to the configured subscribers.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **System > Support > Notifications**.
2. If the default "8:00 AM Daily" delivery time is not acceptable, select the hour, minute, and AM/PM for a new time.
3. Manage the subscriber emails:
 - To add a subscriber, click Add (green plus sign). Enter the email address in the Email Address dialog, and click **Add**.
 - To modify an email address, select the email address in the Subscriber Email list, and click Modify (pencil). Edit the email address in the Email Address dialog, and click **Save**.
 - To delete an email address, select the email address in the Subscriber Email list, and click Delete (X).
4. Click **Apply**.

Managing autosupport reporting

The autosupport reporting feature emails an automatically generated daily report, called an ASUP, to Dell EMC Support.

This report shows DDMC system identification, status information, and entries from various log files. Extensive and detailed internal statistics and information are included at the end of the report to aid support personnel with debugging, if the need arises. However, there is no information about managed systems in this report.

Autosupport reporting is enabled by default. To disable it:

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **System > Support > EMC Support**.
2. Deselect **Auto support and daily alert summary** and/or **Real-time alert**.
3. Click **Apply**.

 **NOTE:** For more information about autosupport reporting, see the *DD OS Administration Guide*.

Using ConnectEMC or legacy email for autosupport

By default, autosupport reports are enabled and sent daily to Dell EMC Customer Support using the *legacy email method*. The *ConnectEMC method* sends messages securely through a Secure Remote Service gateway.

About this task

To determine if autosupport reporting is currently enabled, and if so, the method in use:

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **System > Support > EMC Support**.
2. In the Channel area, select **ConnectEMC**.
3. Add, delete, or change the method priorities.
To change the method, see the *DD OS Administration Guide*.
4. Select the frequency to email the DDMC default administrator.
5. Click **Apply**.

Adding to the autosupport report email list

By default, autosupport reports are enabled and sent daily to Dell EMC Customer Support. You may want to add additional email addresses as recipients of autosupport reports.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **System > Support > Notifications**.
2. In the Autosupport Report dialog, select Add (green + sign) to add an email address.
3. Click **Apply**.

Reviewing generated autosupport reports

The Autosupport Reports panel contains a list of links to current autosupport report files.

To see a generated autosupport report, select a file name link, and view the report using a text editor. If required by your browser, download the file first.

Generating a support bundle manually

When troubleshooting problems, Dell EMC Support may ask you to immediately generate a support bundle, which is a tar-g-zipped selection of log files and a README file that includes identifying autosupport headers.

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **System > Support > Support Bundles**.
2. Click **Generate Support Bundles**.

- When you see the new .tar.gz file, email it to Data Domain Support. If it is too large to be emailed, go to the Dell EMC support site, and upload it.

Managing system logs

A messages file and audit log file are saved on DDMC and listed in the Logs area. Files can be opened and saved to a local location and then forwarded to support, if required.

Steps

- Click the **Settings** button (the gear icon) in the DDMC banner, then select **System > Support > Logs**.
- On the Logs page, view the log file name (which is assigned automatically), the file size, and the date it was last modified. Select a log file name to view its contents. You may be prompted to select an application, such as Notepad.exe, to open the file.
- Save the log file locally, if needed.

Upgrading DDMC software

Only DDMC admins have permission to manage software upgrade packages and perform upgrades for DDMC.

You can upgrade directly to DDMC 7.3 from a system running DDMC 6.1 or later. To upgrade to DDMC 7.3 from a release family earlier than 6.1, you need to upgrade in steps.

Table 36. Direct upgrade

DDMC release	Direct upgrade to:
7.2	7.3
7.1	7.2 or 7.3
7.0	7.1, 7.2, or 7.3
6.2	7.0, 7.1, 7.2, or 7.3
6.1	6.2, 7.0, 7.1, 7.2, or 7.3
2.0	6.1 or 6.2
1.4.5	2.0 or 6.1
1.3	1.4, 1.4.5, or 2.0
1.2	1.3 or 1.4
1.1	1.2 or 1.3

 **NOTE:** The DDMC release family directly after 2.0 is 6.1; there are no 3.x, 4.x, or 5.x versions.

 **NOTE:** The DDMC release family directly after 6.2 is 7.0.

Upgrading DDMC software is done in two stages:

- Obtaining an image from the online support site or selecting a previously obtained upgrade image that has been saved.
- Performing the upgrade on DDMC.

DDMC 7.3 supports management of systems running up to five releases back (DD OS 7.2, 7.1, 7.0, 6.2, and 6.1), and the next two releases when they become available.

Managing DDMC upgrade packages

You can download an upgrade image from the online support site to a locally accessible drive and then add it to the upgrade package collection managed by DDMC.

Steps

1. Click the **Settings** button (the gear icon) in the DDMC banner, then select **System > Upgrade**.
2. In the Upgrade Packages area, view the available upgrade packages, their sizes, and their modification dates. Then, select one of the following options:
 - To get a new upgrade package to store locally, click **Add**, then click the **Online Support** link.
 - To upload a package that has been stored locally to the inventory, click **Add**, then click the **EMC Online Support** link. Browse to the local drive to select the package.
 - To delete a package, select the package from the inventory list, and click **Delete**.
3. To perform the upgrade, see the procedure in the following section.

Performing a DDMC software upgrade

After you have uploaded an upgrade package, you can use it to upgrade your DDMC software.

About this task

 **NOTE:** Software upgrade files use the .rpm file extension. This topic assumes that you are updating only DDMC. If you make hardware changes, such as adding, swapping, or moving interface cards, you must update the DD OS configuration to correspond with the hardware changes.

Steps

1. Review the appropriate release notes for instructions for this upgrade, and verifying available space.
 -  **NOTE:** For most releases, upgrades are permitted from up to two prior major release versions.
2. Click the **Settings** button (the gear icon) in the DDMC banner, then select **System > Upgrade**.
3. In the Upgrade Packages Available area, select the upgrade package from the list, and select **Perform System Upgrade**.
4. Monitor the upgrade progress from the DDMC console page.
5. Be aware that the upgrade process automatically reboots DDMC.
6. It is recommended that you keep the System Upgrade progress dialog open until the upgrade completes, or until the system powers off.

Graphics Reference for DDMC

Topics:

- [Global controls and icons](#)
- [Dashboard controls](#)
- [Widget controls](#)
- [Group icons](#)
- [Property controls](#)

Global controls and icons

The controls and icons that are used throughout the DDMC interface are described in detail.

Table 37. Controls that perform a function

Control	Name	Description
	Alerts	Located in the DDMC banner, shows most recent alerts, a red dot notifies of unseen active alerts
	Help	Located in the DDMC banner and a dropdown menu appears when clicked: <ul style="list-style-type: none"> • About DD Management Center • View EULA • DDMC Guide - This is derived from the <i>PowerProtect DD Management Center Installation and Administration Guide</i>
	User	Located in the DDMC banner and is used to: <ul style="list-style-type: none"> • Display user and role information • Switch to classic view • Logout
	Settings	Located in the DDMC banner and provides direct access to Network, Access, and System settings
	Refresh	Located in the DDMC banner, reloads the page to display latest information
	Filter controls	<p>The filter control is composed of two parts: the funnel icon and a drop-down list.</p> <ul style="list-style-type: none"> • If filtering is being performed, clicking the funnel turns all filtering off, causing all systems to be visible. • If filtering is off, clicking the funnel turns on filtering, using the previously set filter. • When a filter is active, the funnel display is yellow. Click Show Filter or the Filtered by link to see details about what is filtered. <p>Filter selection is performed with the small down arrow, which opens a drop-down list of the types of filtering that can be employed:</p> <ul style="list-style-type: none"> • Filter by group – Enables the selection of one or more groups. Systems belonging to the selected groups display in the work area panel.

Table 37. Controls that perform a function (continued)

Control	Name	Description
		<ul style="list-style-type: none"> • Filter by property – Enables the selection of one or more property values. Systems having those property values display in the work area panel. • Filter by system – Enables the selection of one or more systems to be displayed in the work area panel. • Filter by rule – Enables the creation of a filter rule (or selection of a previously created rule) that controls which systems display in the work area panel. Filter by rule is used to combine systems, groups, and properties to achieve finer granularity. <p> NOTE: You must switch to Classic View in order to use the Filter by rule feature.</p> <ul style="list-style-type: none"> • Filtering is used in the work area panel for monitoring views, but not for Reports and Dashboard widgets.
<ul style="list-style-type: none"> •  •  	System or Group view toggle	<ul style="list-style-type: none"> • View by System (default) – Displays systems as a flat list, whose entries are sortable using the table column sorting controls. • View by Group – Displays systems by their group hierarchy. In this view, sorting of the table is only performed within groups. Group listings can be expanded to a systems list.
	System, Group, Tenant view toggle	<p>Same as the previous icon, but you can also select:</p> <ul style="list-style-type: none"> • View by Tenant – Displays tenants as a flat list, whose entries are sortable using the table column sorting controls.
	Launch DD System Manager	Starts DD System Manager for the selected system, where you can directly manage or investigate the corresponding area from where it was launched.
	Inventory details	Found on Inventory > Upgrades Systems tab under Details column. Icon toggles between hiding and displaying toggles.
	Show columns	Found on many of the views that are table-based, enables the choice of columns that display in the table.
	Column sorter	On table views, sorts the columns in ascending or descending view (by date, alphabetically, by priority, and so on), based on the column datatype.
	Add	Opens a dialog box to add one or more items. The type of item being added depends on the page displayed. For example, on the Inventory > Systems page, this lets you add systems to DDMC. On the Administration > Properties page, this lets you create custom properties for managed objects.
	Edit	For a selected table element, opens a dialog box that allows changing information about the element.
	Delete	Deletes a selected table element.
	Continue	Continues an operation, such as adding another statement when creating a custom rule.

Table 38. Icons showing system and/or connection status

Icon	Status
	Normal – Communication between DDMC and the Data Domain or PowerProtect system is operating normally.
	Unreachable – The system is not responding or is not transmitting. Data was last retrieved as of the date that is shown in the status banner.
	Unmanaged – The system is suspended or unmanaged. When suspended, all data collection ceases. A system is suspended when management has been taken over by another DDMC or when the system is suspended using the CLI.

Table 38. Icons showing system and/or connection status (continued)

Icon	Status
	Adding – The system is being added into the inventory.
	Upgrading – The system is being upgraded and is unavailable during this state.
	Synchronizing – Data for the system is being synchronized. The system is unavailable during this state.
	Unsupported system – This system is unsupported because it is running an operating system that is not supported by this version of DDMC. You may view system details for it, but the data will be out of date. You will see a tooltip with an option to upgrade the system.

Table 39. Icons for Tenants and Tenant Units

Icon	Status
	Tenant Unit Configuration Issues – Reported in all multi-tenancy pages, dialogs, and lightboxes, indicates that this Tenant Unit has no configured alert notification list, no storage provisioned, no hard quota set, and/or no reports configured.

Related tasks

- [Working with filters](#) on page 41
- [Logging into DDMC](#) on page 26

Dashboard controls

The **Dashboard > Monitoring** page consists of from one to seven tabs that you create to hold any number of widgets that provide high-level, quick monitoring views of various aspects of the Data Domain or PowerProtect environment.

Table 40. Dashboard controls

Controls	Name	Description
	Add Dashboard/Tab	Opens the Add Dashboard dialog box
	Add Widget	Opens the Add Dashboard Widget dialog box where you can select a widget template and optional filters to create a widget.
	Add/Configure Tabs	Opens the Add and Configure Dashboard Tabs dialog box where you can add tabs, modify tab names, or delete tabs. You can also set the number of columns and change the ordering of the tabs across the dashboard.
	Maximize/Restore dashboard	Toggles the size of the dashboard. Maximize hides the navigation panel and Restore returns to default view, exposing the navigation panel.

Related tasks

- [Working with filters](#) on page 41

Widget controls

Each widget includes the following standard controls.

Table 41. Widget controls

Controls	Name	Description
	Edit Widget	Opens the Edit Dashboard Widget where you can change the widget name and filter criteria, and in some cases, widget details.

Table 41. Widget controls (continued)

Controls	Name	Description
	Details	The global drill-down button on a widget that navigates to the parent page associated with the widget. For example, for Alerts widgets, the Health > Alerts page is opened.
	Help	Provides information about what the widget monitors and active controls on the widget, such as the control to browse to the parent monitoring page.
	Remove Widget	Deletes the widget from the tab.
 Status	Connection Status	Click Status to open a popup that lists the counts of systems with connection problems in any of these categories: (not responding, not transmitting, suspended, and unmanaged.) Includes a link at the bottom of the popup to browse to the Health > Status page that provides more details about just these systems. NOTE: The Status control displays on a widget when any of the monitored systems (filtered or unfiltered) have one or more connection problems.
	Inactive/Active Table Filter	Indicates that a filter is either inactive or active in a table column where filtering is available.
	Filter	Indicates that a filter is active for the widget.
	Emergency and Alert	When an emergency or alert state is present, click this icon to open the Status > Alerts page to show the emergency/alert messages.
	Critical and Error	When critical or error states are present, click this icon to open the Status > Alerts page to show the critical/error messages.
	Warning	When a warning exists, click this icon to open the Status > Alerts page to show the warning.

Group icons

On the **Administration > Groups** page, the DDMC system administrator creates groups in a tree-like hierarchy for logically organizing Data Domain and PowerProtect systems.

Table 42. Group icons

Controls	Name	Description
	Group	Symbolizes a group containing systems or other groups. When subgroups are present, the expander icon is displayed to the left of the folder. Selecting the folder displays the members of the group in the Group Details panel.
	Group with permissions applied	Indicates that this group is controlled by access permissions.
	Membership details	Appears when a system belongs to more than one group. Hover to view the names of groups of which this system is a member.

Property controls

The controls used to add, edit, and assign properties (**Administration > Properties**) help you quickly see whether a property is a system or user property and help you get more details and information about the property.

Table 43. Property controls

controls	name	description
	System property	Denotes a fixed, pre-set property that cannot be edited. Selecting this control shows all of its created values in the Values column. The default properties, which cannot be modified, are:

Table 43. Property controls (continued)

controls	name	description
		<ul style="list-style-type: none"> ● System – Model, OS, Domain Name ● MTrees – Replicated ● Replication – no default properties
	User property	Denotes a user-defined property. When selected, can be edited or deleted, and all of its created values are shown in the Values column.
	System details	Opens the Property Assignment dialog, which lists the type of property, the name of the element (for example, system name), and assigned value. When opened in the Values column, shows only entities for that value.

Command Line Interface for DDMC

Topics:

- Differences between DDMC CLI and DD OS CLI
- Tasks available only in DDMC CLI
- config template commands
- managed-system commands
- task commands

Differences between DDMC CLI and DD OS CLI

The DDMC CLI (command line interface) was derived from the DD OS CLI, but has been modified to fit the needs and tasks of DDMC.

- There are two unique DDMC commands (`managed-system` and `task`) that perform basic registration, administration, and job management functions.
- Only a subset (fifteen) of the DD OS commands (`adminaccess`, `alerts`, `alias`, `authentication`, `autosupport`, `config`, `help`, `log`, `net`, `ntp`, `route`, `snmp`, `support`, `system`, `user`) are included with DDMC; however, some arguments and output are not included because DDMC does not directly manage storage. The remaining DD OS commands are not included because they are solely concerned with managing storage.

To see the online help for a CLI command in DDMC, start a secure shell session (ssh), and type `?` at the CLI prompt, or type `man command-name`.

Tasks available only in DDMC CLI

It is recommended that you use the DDMC GUI for all system *management* tasks. However, you must use the DDMC CLI for some system *administration* tasks that are not available in the GUI.

- `managed-system resume host`
- `managed-system suspend host`
- `managed-system sync`
- `system show performance [duration duration {hr | min}] [interval interval {hr | min}]`
- `system show serialno detailed`

The GUI shows the current serial number for DDMC, but does not support the detailed version.

- `system show space`
- `system show stats [view {net | iostat | sysstat}] [custom-view view-spec,...] [interval nsecs] [count count]`

config template commands

Configuration efforts of Data Domain and PowerProtect systems with the same or very similar configuration can be minimized by now using the set of `config template` CLI commands to configure groups of systems.

config template apply

This command applies a configuration template to selected protection systems that DDMC manages.

```
config template apply template-name to-managed-systems host-list
```

 **NOTE:** *host-list* is a list of host names managed by DDMC; numeric IP addresses are not allowed.

config template create

This command creates a configuration template from a protection system and saves it in the local database on DDMC.

```
config template create template-name from-managed-system host-name features { all |
adminaccess | alerts | autosupport | config | net | ntp | snmp | feature-list }
[description template-description ]
```

 **NOTE:** Only one host name is allowed.

Table 44. Features and subfeatures for config template

Feature	Sub-feature	Operation
Adminaccess	ssh	Enable/Disable
	ssh hosts	Add/Delete
	scp	Enable/Disable
	telnet	Enable/Disable
	telnet hosts	Add/Delete
	ftp	Enable/Disable
	ftp hosts	Add/Del
	ftps	Enable/Disable
	http	Enable/Disable
	http host	Add/Delete
	https	Enable/Disable
	web-service	Enable/Disable
	web-option http-port	Set/Reset
	Web-option https-port	Set/Reset
Web-option session-timeout	Set/Reset	
Alerts	notify-list group	Create/Delete
	notify-list emails	Add/Delete
	notify-list class severity	Add/Delete
Autosupport	alert-summary	Add/Delete
	alert-summary emails	Add/Delete
	asup-detailed	Add/Delete
	asup-detailed emails	Add/Delete
Config	admin-host	Set/Reset
	admin-email	Set/Reset
	mail-server	Set/Reset
	timezone	Set/Reset
Net	interface	Enable(up)/Disable(down)
	dhcp	Yes/No
	hosts	Add/Delete
	dns	Set/Reset
NTP	time-server	Add/Delete

Table 44. Features and subfeatures for config template (continued)

Feature	Sub-feature	Operation
	status	Enable/Disable
SNMP	status	Enable/Disable
	sys-Contact	Set/Reset
	sys-Location	Set/Reset
	ro-community	Add/Delete
	ro-community hosts	Add/Delete
	rw-community	Add/Delete
	rw-community hosts	Add/Delete
	trap-host	Add/Delete
	user	Add/Delete

config template creation schedule set

This command can be used to set up a daily schedule to create configuration templates for all protection systems DDMC manages.

- A maximum of 3 copies (created by scheduler) per protection system are saved.
- If no configuration is changed from the previous day, a copy is not made.

```
config template creation schedule set { hh:mm | never }
```

config template creation schedule reset

This command resets a daily schedule to stop creating configuration templates for all protection systems DDMC manages.

```
config template creation schedule reset
```

config template destroy

This command destroys a configuration template saved in the local database on DDMC.

```
config template destroy template-name
```

config template rename

This command renames a pre-existing DDMC configuration template.

```
config template rename template-name new-template-name
```

config template show detailed

This command shows the detailed settings of a configuration template that is available for use by the protection systems DDMC manages.

```
config template show detailed [template-name]
```

config template show list

This command shows a list of the configured templates available for use by the protection systems that DDMC manages.

```
config template show list [template-name]
```

managed-system commands

The DDMC `managed-system` CLI commands let you add and remove systems from management, change their proxy host settings, and suspend, resume, or synchronize data collection.

 **NOTE:** You can also use the Web interface to perform these actions.

managed-system add

```
managed-system add hostname [force] [inbound-proxy proxy-host [inbound-proxy-port proxy-port]] [outbound-proxy proxy-host [outbound-proxy-port proxy-port]]
```

This command adds a system to the set of managed systems. The command prompts you to:

1. Verify that the certificate obtained from the host is valid.
2. Type the sysadmin password for the system being added to management.

Argument Definitions

force	If the system is already being managed by another DD Management Center, the current DD Management Center assumes management of the Data Domain system from the other DD Management Center, and the Data Domain system entry in the other DD Management Center is placed in the unmanaged state. If the system is already being managed and you omit this argument, the command fails.
hostname	The host name of the system.
inbound-proxy proxy-host	Inbound proxy host name if the incoming connection from the Data Domain system is through a proxy.
inbound-proxy-port proxy-port	Inbound proxy port number if the incoming connection from the Data Domain system is through a proxy.
outbound-proxy proxy-host	Outbound proxy host name if the connection from the DD Management Center to the Data Domain system is through a proxy.
outbound-proxy-port proxy-port	Outbound proxy port number if the connection from the DD Management Center to the Data Domain system is through a proxy.

 **NOTE:** The proxy options are equivalent to the firewall options in the graphical user interface.

managed-system check-connection

```
managed-system check-connection hostname [inbound-proxy proxy-host [inbound-proxy-port proxy-port]] [outbound-proxy proxy-host [outbound-proxy-port proxy-port]]
```

This command checks whether the specified host is reachable and available to be managed by this DDMC. Use `managed-system add` to add the system to the set of systems that this DDMC is managing.

Argument Definitions

hostname	The host name of the system.
inbound-proxy proxy-host	Inbound proxy host name if the incoming connection from the Data Domain system is through a proxy.
inbound-proxy-port proxy-port	Inbound proxy port number if the incoming connection from the Data Domain system is through a proxy.
outbound-proxy proxy-host	Outbound proxy host name if the connection from the DD Management Center to the Data Domain system is through a proxy.

outbound-proxy-port *proxy-port* Outbound proxy port number if the connection from the DD Management Center to the Data Domain system is through a proxy.

managed-system delete

```
managed-system delete hostname
```

This command removes the specified system from DDMC management.

Argument Definitions

hostname The host name of the system.

managed-system resume

```
managed-system resume hostname
```

This command resumes data collection from the specified system if collection was suspended by `managed-system suspend`.

 **NOTE:** If a system is running an unsupported version of DD OS, it will be resumed, but it will be put back in an unsupported (not suspended) state.

Argument Definitions

hostname The host name of the system.

managed-system set

```
managed-system set hostname [inbound-proxy {proxy-host|none}] [inbound-proxy-port {proxy-port|default}] [outbound-proxy {proxy-host|none}] [outbound-proxy-port {proxy-port|default}]
```

This command sets or changes proxy server information for a managed system.

Argument Definitions

hostname The host name of the system.

inbound-proxy {*proxy-host*|none} Inbound proxy host name if the incoming connection from the Data Domain system is through a proxy. Use `none` to remove the proxy host and clear the proxy port.

inbound-proxy-port *proxy-port* Inbound proxy port number if the incoming connection from the Data Domain system is through a proxy.

outbound-proxy {*proxy-host*|none} Outbound proxy host name if the connection from the DD Management Center to the Data Domain system is through a proxy. Use `none` to remove the proxy host and clear the proxy port.

outbound-proxy-port {*proxy-port*|default} Outbound proxy port number if the connection from the DD Management Center to the Data Domain system is through a proxy. Use `default` to reset the proxy port number.

managed-system show

```
managed-system show [{all | hostname}]
```

This command prints basic information for a list of managed systems or the specified system.

Argument Definitions

- all** Report about all systems. This is the default.
- hostname** The host name of the system.

The report lists the systems by hostname and includes serial number, management state, online status, DD OS version, and latest synchronization time.

Management States

This list describes the possible values of the management `State` column.

- adding** The DDMC is in the process of assuming management of the system.
- deleting** The DDMC is in the process of ending management of the system.
- managed** The DDMC is managing the system.
- suspended** The DDMC is not currently managing and collecting information about the system. Systems go into this state if you use `managed-system suspend` to stop collecting data or a licensing problem prevents data collection.
- unmanaged** The DDMC previously managed the system, but another DDMC has assumed management.
- unsupported** This system is unsupported, because its DD OS version is not supported by this version of DDMC.

Management Status Values of "Managed" Systems

This list describes the possible management `Status` values when a system is in the `managed` state.

- not-responding** DDMC has not been able to send messages to the managed system, or communication has failed in both directions, for more than 30 minutes.
- not-transmitting** The managed system has not responded to messages from DDMC for more than 120 minutes.
- online** Communication with the managed system is normal.
- upgrading** The managed system is in the process of upgrading its DD OS.
- upgrading, not-responding** The managed system is in the process of upgrading its DD OS and is not communicating with DDMC.

managed-system suspend

```
managed-system suspend hostname
```

This command suspends data collection from the specified host. If you do not want DDMC to show a system as unreachable while it is shut down for maintenance, you can use this command to suspend monitoring.

 **NOTE:** If a system is not in a managed state, it cannot be suspended. If a system is running an unsupported version of DD OS, it can be suspended.

Argument Definitions

- hostname** The host name of the system.

managed-system sync

```
managed-system sync
```

This command synchronizes and processes both current and historical data from all managed systems.

task commands

In the CLI, *jobs* are called *tasks*. The DDMC `task` CLI commands let you cancel, pause, resume, and generate reports about jobs. Regular users may work with tasks that they created. The `sysadmin` user may work on all tasks.

The **Health > Jobs** page in the Web interface displays information about jobs that have been initiated from DDMC, including jobs still in progress and jobs that have completed, whether successfully or not. Jobs include actions such as adding and removing systems from management.

task cancel

```
task cancel task-id
```

This command terminates a task.

Argument Definitions

task-id The ID number for the task, as reported by one of the `task show` commands.

task pause

```
task pause task-id
```

This command suspends a task. Use `task resume` to continue the task.

Argument Definitions

task-id The ID number for the task, as reported by one of the `task show` commands.

task resume

```
task resume task-id
```

This command continues a task that you suspended with `task pause`.

Argument Descriptions

task-id The ID number for the task, as reported by one of the `task show` commands.

task show active

```
task show active [type {inventory | replication | upgrade}] [user user]
```

This command reports about top-level running tasks. You can filter the results by using `type` with one of the keywords, or with the `user` keyword.

Argument Definitions

type {**inventory** | **replication** | **upgrade**}

user *user* Filter the results to show only tasks owned by the specified user.

task show detailed

```
task show detailed task-id
```

This command prints a detailed report about the inputs and outputs of a task in the form of key-value list.

Argument Definitions

task-id The ID number for the task, as reported by one of the `task show` commands.

task show detailed-active

```
task show detailed-active [type {inventory | replication | upgrade}] [user user]
```

This command prints a detailed report about active tasks and their subtasks. You can filter the results by using `type` with one of the keywords, or with the `user` keyword.

Argument Definitions

type {**inventory** | **replication** | **upgrade**}

user *user* Filter the results to show only tasks owned by the specified user.

task show detailed-history

```
task show detailed-history [last n {hours | days | weeks | months}] [start MMDDhhmm[[CC]YY]  
end MMDDhhmm[[CC]YY] [type {inventory | replication | upgrade}] [user user]
```

This command prints a detailed report about completed tasks and their subtasks. You can filter the results by using `type` with one of the keywords, or with the `user` keyword. You can filter the results by time by using the `last`, `start`, and `end` keywords. The default reporting period is the past 24 hours.

Argument Definitions

last *n* {**hours** | **days** | **weeks** | **months**}

start *MMDDhhmm*[[*CC*]*YY*] **end** *MMDDhhmm*[[*CC*]*YY*]

Filter the results to show only tasks that finished during the specified interval. *MMDD* indicates month and day. *hhmm* indicates hours and minutes in 24-hour format. To specify midnight between Sunday night and Monday morning, use **mon 0000**. To specify noon on Monday, use **mon 1200**. *CC* is the first two digits of the year. *YY* is the last two digits of the year.

type {**inventory** | **replication** | **upgrade**}

user *user* Filter the results to show only tasks owned by the specified user.

task show history

```
task show history [last n {hours | days | weeks | months}] [start MMDDhhmm[[CC]YY] end  
MMDDhhmm[[CC]YY] [type {inventory | replication | upgrade}] [user user]
```

This command prints a brief report about completed tasks. You can filter the results by using `type` with one of the keywords, or with the `user` keyword. You can filter the results by time by using the `last`, `start`, and `end` keywords. The default reporting period is the past 24 hours.

Argument Definitions

last *n* {hours | days | weeks | months} Filter the results to show only tasks that finished during the previous *n* hours, days, weeks, or months.

start *MMDDhhmm*[[*CC*]*YY*] end *MMDDhhmm*[[*CC*]*YY*] Filter the results to show only tasks that finished during the specified interval. *MMDD* indicates month and day. *hhmm* indicates hours and minutes in 24-hour format. To specify midnight between Sunday night and Monday morning, use **mon 0000**. To specify noon on Monday, use **mon 1200**. *CC* is the first two digits of the year. *YY* is the last two digits of the year.

type {inventory | replication | upgrade} Filter the results to show only tasks of the specified type.

user *user* Filter the results to show only tasks owned by the specified user.