EMC® Data Domain®
Management Center
Version 1.3

User Guide
302-001-661
REV 01
# CONTENTS

<table>
<thead>
<tr>
<th>Preface</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Chapter 1</strong> DD Management Center Overview</td>
<td>11</td>
</tr>
<tr>
<td>Introducing DD Management Center</td>
<td>12</td>
</tr>
<tr>
<td>Features of DD Management Center</td>
<td>12</td>
</tr>
<tr>
<td>Differences between DD Management Center and DD System Manager</td>
<td>13</td>
</tr>
<tr>
<td>Backing up and restoring in a VMware environment</td>
<td>13</td>
</tr>
<tr>
<td><strong>Chapter 2</strong> Getting Started</td>
<td>15</td>
</tr>
<tr>
<td>Logging in and out of DD Management Center</td>
<td>16</td>
</tr>
<tr>
<td>Logging in to DD Management Center</td>
<td>16</td>
</tr>
<tr>
<td>Logging out of DD Management Center</td>
<td>16</td>
</tr>
<tr>
<td>Understanding RBAC in DD Management Center</td>
<td>16</td>
</tr>
<tr>
<td>Viewing DD Management Center page elements</td>
<td>17</td>
</tr>
<tr>
<td>Navigating a DD Management Center page</td>
<td>18</td>
</tr>
<tr>
<td>Organizing the dashboard</td>
<td>18</td>
</tr>
<tr>
<td>Adding tabs</td>
<td>19</td>
</tr>
<tr>
<td>Adding widgets</td>
<td>19</td>
</tr>
<tr>
<td>Copying tabs</td>
<td>21</td>
</tr>
<tr>
<td>Modifying widgets</td>
<td>22</td>
</tr>
<tr>
<td>Organizing managed DD systems</td>
<td>22</td>
</tr>
<tr>
<td>Creating groups</td>
<td>22</td>
</tr>
<tr>
<td>Adding properties to systems, MTrees, replication pairs</td>
<td>23</td>
</tr>
<tr>
<td>Adding (registering) DD systems to DD Management Center</td>
<td>24</td>
</tr>
<tr>
<td>Inbound and outbound proxy host names and port numbers used by the firewall</td>
<td>25</td>
</tr>
<tr>
<td>Editing DD system settings</td>
<td>27</td>
</tr>
<tr>
<td>Assigning properties</td>
<td>28</td>
</tr>
<tr>
<td>Assigning system property values</td>
<td>28</td>
</tr>
<tr>
<td>Assigning replication property values</td>
<td>29</td>
</tr>
<tr>
<td>Assigning MTree property values</td>
<td>29</td>
</tr>
<tr>
<td>Displaying property information</td>
<td>29</td>
</tr>
<tr>
<td>Displaying properties for an element</td>
<td>29</td>
</tr>
<tr>
<td>Finding elements by property value</td>
<td>30</td>
</tr>
<tr>
<td>Managing groups</td>
<td>30</td>
</tr>
<tr>
<td>Managing replication lag threshold policies</td>
<td>31</td>
</tr>
<tr>
<td>Working with filters</td>
<td>31</td>
</tr>
<tr>
<td><strong>Chapter 3</strong> Monitoring Data Domain Systems</td>
<td>33</td>
</tr>
<tr>
<td>How DD Management Center helps you monitor DD systems</td>
<td>34</td>
</tr>
<tr>
<td>Data retention policy for DD Management Center</td>
<td>34</td>
</tr>
<tr>
<td>Space projection algorithm for DD Management Center</td>
<td>35</td>
</tr>
<tr>
<td>Performing daily monitoring</td>
<td>35</td>
</tr>
<tr>
<td>Checking dashboard status widgets</td>
<td>36</td>
</tr>
<tr>
<td>Checking alert notifications</td>
<td>37</td>
</tr>
<tr>
<td>Checking health status</td>
<td>37</td>
</tr>
<tr>
<td>Checking health alerts</td>
<td>38</td>
</tr>
</tbody>
</table>
Chapter 4 Managing Data Domain Systems

Launching DD System Manager
Upgrading DD system software
Managing DD system upgrade packages
Performing a DD system upgrade
Creating access for users
Understanding DD Management Center permissions

Chapter 5 Administering Secure Multitenancy

How DD Management Center helps with SMT monitoring
Data Domain Secure Multitenancy overview
Managing Tenant users and their privileges
Using DD Management Center to administer SMT
Creating and managing Tenants
Creating Tenants
Viewing Tenant information and status
Tenant Details lightbox
Editing Tenant information
Deleting Tenants
Creating and managing Tenant Units
Creating a new Tenant Unit with the wizard
Viewing Tenant Unit information and status
Tenant Unit Details lightbox
Editing Tenant Unit information
Deleting Tenant Units and unassigning provisioned storage
Adding an unmanaged Tenant Unit to a Tenant
Creating, editing, and generating reports for SMT
SMT report permission table
Creating report templates for SMT
Editing report templates
Generating reports

Chapter 6 Performing Additional Configuration

Managing access to DD Management Center
Roles required for DD Management Center tasks
Managing administrator access
Managing local user access to DD Management Center
Configuring authentication
Viewing active users
Managing network settings
Configuring network interfaces
<table>
<thead>
<tr>
<th>Appendix A</th>
<th>Graphics Reference for DD Management Center</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Global controls and icons..................</td>
</tr>
<tr>
<td></td>
<td>Dashboard controls..........................</td>
</tr>
<tr>
<td></td>
<td>Widget controls.............................</td>
</tr>
<tr>
<td></td>
<td>Group icons....................................</td>
</tr>
<tr>
<td></td>
<td>Property controls...........................</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Appendix B</th>
<th>Command Line Interface for DD Management Center</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Differences between DDMC CLI and DD OS CLI.....</td>
</tr>
<tr>
<td></td>
<td>Tasks available only in DDMC CLI................</td>
</tr>
<tr>
<td></td>
<td>managed-system commands.........................</td>
</tr>
<tr>
<td></td>
<td>managed-system add................................</td>
</tr>
<tr>
<td></td>
<td>managed-system check-connection................</td>
</tr>
<tr>
<td></td>
<td>managed-system delete...........................</td>
</tr>
<tr>
<td></td>
<td>managed-system resume...........................</td>
</tr>
<tr>
<td></td>
<td>managed-system set................................</td>
</tr>
<tr>
<td></td>
<td>managed-system show.............................</td>
</tr>
<tr>
<td></td>
<td>managed-system suspend.........................</td>
</tr>
<tr>
<td></td>
<td>managed-system sync............................</td>
</tr>
<tr>
<td></td>
<td>task commands....................................</td>
</tr>
<tr>
<td></td>
<td>task cancel......................................</td>
</tr>
<tr>
<td></td>
<td>task pause.......................................</td>
</tr>
<tr>
<td></td>
<td>task resume......................................</td>
</tr>
<tr>
<td></td>
<td>task show active................................</td>
</tr>
<tr>
<td></td>
<td>task show detailed.............................</td>
</tr>
<tr>
<td></td>
<td>task show detailed-active.....................</td>
</tr>
<tr>
<td></td>
<td>task show detailed-history....................</td>
</tr>
<tr>
<td></td>
<td>task show history................................</td>
</tr>
</tbody>
</table>
As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The release notes provide the most up-to-date information on product features.

Contact your EMC technical support professional if a product does not function properly or does not function as described in this document.

Note
This document was accurate at publication time. Go to EMC Online Support (https://support.emc.com) to make sure that you are using the latest version of this document.

Purpose
This guide describes how to use EMC Data Domain Management Center (DD Management Center) features and tools.

This guide should be used after completing the instructions in the *EMC Data Domain Management Center Initial Configuration Guide*.

Audience
This guide is intended for use by both system administrators and general users of DD Management Center.

Related documentation
The following EMC publications provide additional information:
- *EMC Data Domain Management Center Initial Configuration Guide*
- *EMC Data Domain Management Center Version Support Matrix*
- *EMC Data Domain Management Center Release Notes*
- For additional information about EMC Data Domain systems, see:
  - The EMC Data Domain Operating System software documentation set.
  - The EMC Data Domain system installation and setup guides for each of your Data Domain platforms.

Special notice conventions used in this document
EMC uses the following conventions for special notices:

**NOTICE**

A notice identifies content that warns of potential business or data loss.

Note
A note contains information that is incidental, but not essential, to the topic.

Typographical conventions
EMC uses the following type style conventions in this document:

**Bold** Indicates interface elements, such as names of windows, dialogs, buttons, fields, tab names, key names, and menu paths
Where to get help
Information about EMC software documentation, product updates, support, licensing, and more can be found at EMC Online Support (https://support.emc.com).

EMC Data Domain product documentation
To view documentation for EMC Data Domain products, go to EMC Online Support (https://support.emc.com), and select Support by Product below the Search box. Type Data Domain in the Find a Product box, wait for those words to appear in the list of matches below the box, and select the words. Then select ». In the list of categories under the Search box, select Documentation.

- The Product choices let you filter results by Data Domain system model number, such as DD990, or by DD OS software release.
- The Content Type choices let you filter results by category. Select More under Content Type to see all of the categories. The categories that contain end-user and compatibility documentation are:
  - Manuals and Guides, for the software and hardware manuals for your system, and for integration guides that explain how to use EMC Data Domain systems with backup software and other products
  - Release Notes, for specific versions of the EMC Data Domain Operating System and EMC Data Domain products
  - Compatibility Document, for guides that show which EMC and third-party components are compatible

Technical support
From EMC Online Support (https://support.emc.com), select Service Center. You will see several options for contacting EMC Technical Support. To open a service request, you must have a valid support agreement. Contact your EMC sales representative to get a valid support agreement or for questions about your account.

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

Changes made to each revision of this guide are listed below.

<table>
<thead>
<tr>
<th>revision</th>
<th>date</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>May 2015</td>
<td>This revision includes information about the following new features of DD Management Center 1.3:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• New Tenant and Tenant Unit views for Capacity and Replication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configuration of per Storage Unit DD Boost Stream Limits</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Access Control-based visibility of Tenant and Tenant Unit content</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unmanaged Tenant Unit editing and assignment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Native IPv6 support throughout the user interface</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Kerberos Token-based Authentication support</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unsupport DD OS version handling</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Password policy enforcement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ConnectEMC configuration monitoring</td>
</tr>
</tbody>
</table>

The following commands have changed in this release:

- **managed-system resume**: 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.
- **managed-system show**: The output now has a new possible state: unsupported.
- **managed-system suspend**: If a system is running an unsupported version of DD OS, it can be suspended.
Preface
CHAPTER 1

DD Management Center Overview

- Introducing DD Management Center ................................................................. 12
- Features of DD Management Center ................................................................. 12
- Differences between DD Management Center and DD System Manager .......... 13
- Backing up and restoring in a VMware environment ......................................... 13
Introducing DD Management Center

*Data Domain Management Center* is a scalable, virtual appliance-based solution for centralized management of multiple *Data Domain systems*.

- DD Management Center provides current and historical data for all of your managed DD systems, with subject presentation ranging from site-wide summaries to drill-down detail for a selected object.
- DD Management Center can configure and monitor secure multitenant DD Boost backup and replication storage on multiple DD systems.
- DD Management Center, a RIA (rich Internet application), is comprised of a set of browser-based pages and is installed and runs on a VMware system (as described in the *EMC Data Domain Management Center Initial Configuration Guide*).

Features of DD Management Center

The robust features of DD Management Center help you work with all of your managed DD systems through one convenient graphical user interface.

These features enable you to:

**monitoring and managing:**
- Monitor the health and operation of managed objects on a user-defined dashboard
- Display site-wide storage capacity, showing aggregated usage totals
- 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 when replications lag
- Manage user access through configurable RBAC (role-based access control) settings

**estimating and reporting:**
- 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, viewed from a single list, for all of your managed DD systems

**grouping and working with multiple DD systems:**
- Open a DD System Manager session for each managed DD system, simultaneously providing both advanced multiple-system management capabilities with DD Management Center and full single-system management capabilities with DD System Manager
- Create custom groupings of your managed DD systems, organized efficiently and intentionally. Applying groups and properties to managed objects lets you customize how content will be displayed, to best represent your infrastructure.
- Configure any and all features for your managed DD systems individually or in groups, such as user access and DD OS upgrades
Differences between DD Management Center and DD System Manager

DD Management Center differs from DD System Manager in the following ways:

- DD Management Center can manage many more DD systems (up to 100) than DD System Manager. DD System Manager is primarily a single-system management tool that provides centralized monitoring and management for up to 20 systems.
- DD Management Center can perform tasks on groups of DD systems, simultaneously.
- DD Management Center aggregates storage and performance data, as well as compares operational information, for all managed DD systems. DD System Manager does not aggregate storage and/or performance data from multiple systems, nor can you compare operational information across systems.
- DD Management Center does not directly manage storage. DD System Manager does directly manage storage (using VTL, CIFS, NFS, DD Boost, and so on).

Backing up and restoring in a VMware environment

Any process that creates and restores a snapshot of your entire virtual machine can successfully protect your DD Management Center installation.

It is highly recommended that you perform a snapshot of your virtual machine before doing an upgrade procedure.

DD Management Center does not depend on having any integration with the backup software.

After the snapshot is restored, DD Management Center automatically performs any necessary application recovery.

Suitable backup software choices would include VDR (VMware Data Recovery), EMC Avamar, etc.

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

Note

The use of cloning has not been validated.
CHAPTER 2

Getting Started

- Logging in and out of DD Management Center ....................................................... 16
- Understanding RBAC in DD Management Center .................................................... 16
- Viewing DD Management Center page elements .................................................... 17
- Navigating a DD Management Center page ............................................................ 18
- Organizing the dashboard ..................................................................................... 18
- Organizing managed DD systems .......................................................................... 22
- Assigning properties ............................................................................................. 28
- Displaying property information ............................................................................ 29
- Managing groups .................................................................................................. 30
- Managing replication lag threshold policies .......................................................... 31
- Working with filters ............................................................................................... 31
Logging in and out of DD Management Center

DD Management Center is accessed by using a supported browser on a workstation that has network access to the hosting VMware server. DD Management Center supports multiple simultaneous users.

The following browsers are supported for use with DD Management Center:

- On Microsoft Windows – Microsoft Internet Explorer 9, 10, or 11; 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 *EMC Data Domain Management Center Release Notes* for the most up-to-date information.

Note

If DD Management Center is not already installed on the VMware server, refer to the *EMC Data Domain Management Center Initial Configuration Guide* for instructions.

Logging in to DD Management Center

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 DD Management Center) may login.

To log in to DD Management Center:

Procedure

1. Open a browser, and enter the host name or IP address of DD Management Center. 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 DD Management Center, the Dashboard is displayed, showing the default set of monitoring widgets.

Logging out of DD Management Center

To log out of DD Management Center, select the Log out button (right-pointing arrow at the top right of the banner), or just close your browser window.

Understanding RBAC in DD Management Center

DD Management Center uses RBAC (role-based access control) to control how data is manipulated and displayed both within DD Management Center and on DD systems managed by DD Management Center.

DD Management Center users can:
• Have one of two roles within DD Management Center: *admin* (system administrator) or *user* (basic user)
• Have one of three roles on the DD systems managed by DD Management Center: *sysadmin* (system administrator), *user* (basic user), or *backup operator*
• Modify DD Management Center states only if they have the *admin* role
• View data from a DD system (through DD Management Center) as permitted by the role they have on that DD system
• Modify a DD system only if they have the *sysadmin* role on that DD system

**Viewing DD Management Center page elements**

DD Management Center is comprised of a variety of page elements.

1. Navigation Panel
2. Banner
3. Widget (this is the Current Health Status widget)
4. Logout Control
5. Online Help Control
6. Module (this is the Replication module)
7. Work Area
8. Status Bar and Notification Area

Unless the dashboard is maximized, the banner is visible at all times and provides controls to filter the scope of the work area’s active page (the filter control appears only on monitoring pages), open the online help, and log out.

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.
The status bar shows the active user name and role, date, and alerts notifications (which you can select, to see an informational pop-up with a link to the Alerts page). Standard global controls (add, edit, delete) allow interaction with the application and manage how information is displayed on pages with tables (sorting column content by ascending/descending controls, hiding/displaying columns).

Navigating a DD Management Center page

Navigation elements on a DD Management Center page change the focus and scope of the content displayed in the work area.

1. Module topics are found on the left, in the navigation panel. The default view opens in the work area. In this picture, you have selected the **Capacity > Utilization** module.
2. Tabs (if applicable) are found at the top right, in the banner. In this picture, you can choose from a **System** or **MTree** view.
3. Toggle buttons (if applicable) let you change from a standard DD system list, to a group of systems, to a Tenant view, etc. 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.

Organizing the dashboard

The Dashboard holds *widgets* that you create from a set of monitoring functions. The Dashboard lets you quickly check important conditions, such as unreachable systems, active alerts, diminishing capacity, etc. 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 a set of systems based on group membership, location, OS version, data type, etc. 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, populated by one each of the supplied widgets, configured to cover all of 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. Up to seven tabs are allowed.

### Adding tabs

To customize your DD Management Center setup, you can add tabs – choosing a unique name, number of columns, and placement.

**Procedure**

1. Select **Dashboard > Monitoring**.
2. On the dashboard, select the **Add tab** control in the banner, at the top right.
3. In the Add and Configure Dashboard Tabs dialog, select Add (green plus sign).
4. In the highlighted text field, enter the name for the tab.
5. Choose the number of columns for the tab (more columns produce smaller widgets).
6. Order the placement of the tab across the dashboard using the **Move Up** or **Move Down** controls.
7. Select **Save**.

**Results**
The new tab is displayed on the dashboard.

### Adding widgets

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

**Procedure**

1. Select **Dashboard > Monitoring**.
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 Top Replication Lags template, you could name the widget “New Jersey Replication Lag” 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 icon 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. Select **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.

**Current Health Status widget**

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

Selecting the Show detail control (>>) takes you to 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.

Color-coded bar graphs for severity levels show alert totals and the number of systems affected.

Selecting the Show detail control (>>) takes you to the Health > Alerts page, where a complete list of Health Alerts is displayed.

**Capacity Overview widget**

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

Color-coded bars show critical, warning, and normal capacity levels.

A configuration option lets you show projected capacity usage for a selected period of time (from 1 to 18 months).

Selecting the Show detail control (>>) takes you to the Capacity > Utilization page.

**Space Usage widget**

The **Space Usage** widget shows summaries of capacity factors – total space, space used, space available, pre-comp(ression) space used, and compression ratio.

It also displays alerts for systems at capacity and warnings for those nearing capacity.

Selecting the Show detail control (>>) takes you to the Capacity > Utilization page.

**Replication Status widget**

The **Replication Status** widget shows a summary of important status factors for replication pairs.

This widget shows the number of replications being monitored, the number of source and destination systems or groups, and data transfer totals. If any pairs have critical or warning status, a warning icon displays, which when selected, opens the appropriate Replication page.

Configuration options include setting the widget to monitor only Automatic or only On-Demand replications. Additional options allow selecting specific replication status factors (such as pre-comp bytes written in the last 24 hours) for Automatic replications or file transfer status for the last 24 hours when configuring On-Demand replications.

Selecting the Show detail control (>>) takes you to the Replication > Automatic page.
Note
For DD Boost (on-demand replication) monitoring, the DD system must be running DD OS 5.3.1 or later. Any DD system running older software will not display DD Boost replication pair associations between the source and destination systems on any of the file replication reporting pages, widgets, or reports.

Top Replication Lags widget
The Top Replication Lags widget shows a list of systems exhibiting the longest lag time. Selecting the Show detail control (>>) takes you to the Replication > Automatic page, where the complete list of filtered DD systems with lagging replications is shown, and you can view or change the Lag Threshold Policy. Selecting a row in the widget takes you to the Replication > Automatic page, filtered to show only those pairs whose source is the selected system.

Note
For DD Boost (on-demand replication) monitoring, the DD system must be running DD OS 5.3.1 or later. Any DD system running older software will not display DD Boost replication pair associations between the source and destination systems on any of the file replication reporting pages, widgets, or reports.

Replication Lag Status By Pairs widget
The Replication Lag Status By Pairs widget shows the count of replications with critical, warning, and normal levels, based on the Lag Threshold Policy. Selecting the Show detail control (>>) takes you to the Replication > Automatic page, where the list of all filtered replications is shown, and you can view or change the Lag Threshold Policy.

Note
For DD Boost (on-demand replication) monitoring, the DD system must be running DD OS 5.3.1 or later. Any DD system running older software will not display DD Boost replication pair associations between the source and destination systems on any of the file replication reporting pages, widgets, or reports.

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

Procedure
1. Select Dashboard > Monitoring.
2. Select the Add tab control in the banner, at the top 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. Select **Save**.

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

---

**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 DD systems**

When you add DD systems to DD Management Center, the “Add systems” wizard includes options to assign each system to a group, or groups, and to set properties for it.

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

- Groups can be applied only to DD systems.
- Properties can be applied to DD systems, MTrees, and replication contexts.
- A default set of system properties (DD system model, DD OS version, domain name, and data center) is automatically assigned when a system is added, so you will need to set only *custom* properties. You can also modify (but not delete) data center properties, as needed.

After you have completed the initial setup for each DD system, you can continue to add and edit values for properties, and you can assign and reassign group membership.

---

**Creating groups**

Groups are ways to organize DD systems under a specific name, in a hierarchical structure created by the DD Management Center administrator.

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

---

**Note**

DD systems cannot be added at the root Groups node. Group hierarchy structures cannot be changed; they must be deleted and re-created to change the structure.

---

**Procedure**

1. Select **Administration** > **Groups**.
2. To add a group at the root level, select Add (green plus sign).
3. Make sure only the “/” is in the Path box. Enter a name for the new group, and select Save.

The /newgroup is listed in the Groups panel.

4. To add a sub-group to a group, select a group (which will be the parent group) from the Groups panel, select Add (green plus sign), enter a name for the sub-group, and select Save.

The sub-group is nested under the parent group in the Groups panel.

5. After a DD system has been added to DD Management Center, it can be added to a group. Select the target group from the Groups panel, and select Add (green plus sign). In the Add Group dialog, select a DD system from the Available Systems panel, select > to move the system into the Systems in the Group panel, and select Save.

The DD system is displayed in the Group group name Details panel when the group is selected in the Groups panel. When a DD 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, MTrees, replication pairs

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

Procedure

1. Select Administration > Properties.

2. At top right, select one of the tabs (System, MTree, or Replication), and select Add (green plus sign).

3. In the Add Property dialog, enter 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.

4. Select Add.

5. Assign values to the properties, as described in “Assigning Properties”.

Getting Started
Adding (registering) DD systems to DD Management Center

Before you can manage a DD system in DD Management Center, you must add (register) it to the inventory. A maximum of 100 DD systems can be added to a DD Management Center. Groups of up to 20 systems can be registered at one time.

Procedure

1. Select Inventory > Systems.

2. Select Add (green plus sign). Enter the following for the first DD system, then select Add to continue adding systems (up to 20 systems total). Make sure the box next to the system being added is checked. Select Register to continue:

- **Host name** (required) – Enter the fully-qualified host name (use alphanumeric characters, dashes, periods, and underscores) or IP address. Ensure that the host name and the DNS name for the DD system match; a mismatch may cause problems with backup software.
- **Sysadmin Password** (required) – Enter the sysadmin password used on the DD system (required).
- **Firewalls** (optional) – Enter the inbound and outbound proxy host name (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 DD Management Center communicate with the DD system. If the ports have been changed on the firewall or the DD system, they should also be updated here.

**Note**

For more detailed information, see the next section, Inbound and outbound proxy host names and port numbers used by the firewall on page 25.

- **Certificate** (optional) – Check certificate information by clicking in the associated cells. The Subject name in the DD Management Center CA certificate should match the DD Management Center host name, or SSL will fail the host verification.

3. The status page reports the success and/or failure of the additions. In the event of an error, select Back to return to the first page to display error messages and correct errors, or to delete the system. When you have fixed all of the errors, select Next to continue to the Properties page or Close to quit. (The Next button will be disabled until all of the errors are corrected.)

**Note**

Any settings made on the Properties page, the Groups page, and the Thresholds page will be applied to all of the systems being added.

4. Optionally, on the Properties page, select checkboxes from the available properties list to assign properties to the DD systems, and select Next to continue to the Groups page.

5. Optionally, on the Groups page, select checkboxes from the available groups list to make all DD systems members of the selected groups, and select Next to continue to the Thresholds page.

6. Optionally, on the Thresholds page, set warning and critical capacity thresholds for the DD systems (shown on capacity views and in reports).
7. Select Finish.

Results

A progress bar appears on the page showing the progress of the initial data synchronization for the newly added DD system(s). Additionally, job progress details can be tracked on the Health > Jobs page.

After a DD system is added to DD Management Center, all historical information for that DD system is copied to DD Management Center. From that point on, whenever operational data changes on that DD system, the DD system notifies DD Management Center, which immediately polls the DD 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 DD system to DD Management Center:

- Make sure the DD system is online. A DD system must be online in order to be added to DD Management Center.
- If you specified a port number in the proxy firewall settings, make sure it is correct.
- Make sure you have added the DD Management Center to the DD system as a host.
- Make sure there are no networking issues preventing communication between the DD Management Center and the DD system.
- If you specified a host name for the DD system, make sure the host name can be resolved in your name space (DNS).
- Make sure the password entered for the system is correct.
- Make sure the DD OS version of the DD system is supported by your current version of DD Management Center (see the EMC Data Domain Management Center Version Support Matrix).
- Make sure the DD system is not already managed by another DD Management Center. To resolve this, you can either delete the system from the original DD Management Center or select the Override adding systems checkbox. The system will be added to the new DD Management Center, but the system’s status will be changed to unmanaged on the original DD Management Center, and data collection will be suspended for that system.

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

Firewalls provide an additional level of security when transmitting data between DD Management Center and DD systems. You must set inbound and outbound proxy host names (or IP addresses) and port numbers for a firewall if the connection between DD Management Center and the DD system is through a proxy.

The terms inbound and outbound are from the perspective of DD Management Center, so inbound means from the DD system to DD Management Center, and outbound means from DD Management Center to the DD 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.

DD Management Center connecting directly to a DD system (simple case)

In the simplest case of connecting DD Management Center to a DD system, the DD system is able to resolve "dmc.myco.com" to 1.1.1.1, and DD Management Center is able to resolve "drr.myco.com" to 1.1.1.2.
**Figure 1** Simple case: DD Management Center connecting directly to a DD system

In this simplest case, it is assumed that:

- DD Management Center is able to connect to the DD system using TCP.
- The DD system is similarly able to connect to DD Management Center using TCP.
- DD Management Center, by default, tries to translate the host name of a DD 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 DD system similarly tries to translate the DD Management Center host name to an IP address using DNS or a host file.
- Both DD Management Center and DD OS (on the DD system) try to connect to port 3009 on the remote system.

**DD system with multiple network interfaces**

When a DD system has multiple network interfaces, you need control of the specific interface used by DD Management Center.

**Figure 2** DD system with multiple network interfaces

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

**NAT firewall between DD Management Center and DD system**

When a NAT (network address translation) firewall exists between DD Management Center and a DD 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 DD Management Center connects does not match any IP address on the DD system, itself. Port numbers may be re-mapped, as well. Therefore, to connect to a DD system, you would connect to a port other than 3009 on the proxy.
In this case, when DD Management Center wants to connect to port 3009 on the DD system, DD Management Center must actually try to connect to port 12,345 on the firewall. Conversely, when the DD system wants to connect to port 3009 on DD Management Center, the DD system must actually try to connect to port 54,321 on the other side of the firewall.

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

**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 host name of the DD Management Center, or the host name of the DD 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 DD Management Center in the inbound proxy host name field and/or the IP address of the DD system in the outbound proxy host name field.

**Editing DD system settings**

After DD systems have been added to DD Management Center, you can edit their configuration settings, properties, group assignments, and thresholds.

**Procedure**

1. Select **Inventory > Systems**.
2. Select one or more DD systems and then Edit (yellow pencil).
3. In the Edit System(s) dialog, choose any or all of the tabs to make changes (select **Apply**, or change tabs to save the new settings and continue reconfiguration). If you selected more than one DD system, only the Properties and Thresholds tabs are available.

- **Configuration** lets you edit the inbound and outbound proxy host name (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 DD Management Center communicate with the DD system. If the ports have been changed on the firewall or the DD system, they should also be updated here.
Note

For more detailed information, see the previous section, Inbound and outbound proxy host names and port numbers used by the firewall on page 25.

- **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, OS, 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 DD system.

- **Groups** let you organize DD systems under a specific name, in a hierarchical structure created by the DD Management Center administrator, which is helpful for searches. You can add or remove group assignments, and select or deselect group assignments for the system. Any number of groups and subgroups can be selected.

- **Thresholds** indicate the warning and critical capacity thresholds for DD systems 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: DD systems, replication, or MTrees.

### Assigning system property values

After you add a property to a DD system (Administration > Properties > System), you can assign values to that property.

**Procedure**

1. Select Inventory > Systems.
2. Select one or more systems.
3. Select Edit (yellow pencil), and in the Edit System dialog, select the Properties tab.
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 will show *Mixed values*. If you change the value, all systems will 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 – 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.
5. Select OK to set the values.
Assigning replication property values

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

Procedure
1. Select Replication › Overview or 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. Select Assign to set the values.
5. To see values 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 assigned to a context will appear in the cell.

Assigning MTree property values

After you add an MTree property (Administration › Properties › MTree), you can assign values to that property.

Procedure
1. Select Capacity › Utilization › MTree tab.
2. At bottom right, in Properties, select Assign 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.
3. Select Assign to set the value.

Displaying property information

Assigned property values can be displayed either by selecting an element (such as a DD system) and displaying all of the properties assigned to it, or by selecting a property and displaying all of the elements to which it is assigned.

Displaying properties for an element

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

Procedure
- Systems – Select Inventory › Systems, and select a DD 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, uncheck the property from the list. Some properties may not be removed from the table, so they will not appear in the list of configured properties under the gear control.

- **Replication** – Select Replication > Overview, select a replication pair, and select Pair Details.
  Any properties assigned to the replication pair are displayed in the Properties panel.
- **MTree** – Select Capacity > Utilization, select the MTree tab, and select an MTree.
  Any properties assigned to the MTree are displayed in the Properties panel.

### Finding elements by property value

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

**Procedure**

1. Select Administration > Properties, and select the property type (System, MTree, 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.

### Managing groups

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

Any permissions that are applied to a group affect all DD 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 DD systems to existing groups.
- Use **Delete** to remove DD 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 DD 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.

By assigning a replication lag threshold policy, you are assured that notifications will be displayed in the Replication > Automatic page and the Top Replication Lags and Replication Lag Status widgets 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.

Procedure
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 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. Select Save.
4. Back in the Lag Threshold Policy dialog, select a policy from the Threshold Policy menu, and select 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 DD Management Center 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 DD systems to be monitored for Dashboard widgets. The Filter (funnel-shaped) control appears on pages and dialogs whenever a filter can be used.

The drop-down menu on the Filter control allows you to select the groups, properties, DD systems, or rules to be used for filtering. When a filter is active on a page, the Filter control is highlighted in yellow. 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, DD systems), along with any existing properties or groups that have been created. Controls for logic (is, is not, contains, does not contain, etc.) are provided, and statements can be inclusive or selective.

To create a custom filter rule:

**Procedure**

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 that the filter may still be available with the **Recent filters** option on the Filter control list.
CHAPTER 3

Monitoring Data Domain Systems

- How DD Management Center helps you monitor DD systems ........................................... 34
- Data retention policy for DD Management Center .......................................................... 34
- Space projection algorithm for DD Management Center .............................................. 35
- Performing daily monitoring ....................................................................................... 35
- Monitoring capacity ....................................................................................................... 40
- Checking the System Details lightbox .......................................................................... 42
- Monitoring replication .................................................................................................... 43
- Monitoring status with reports ..................................................................................... 47
How DD Management Center helps you monitor DD systems

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

After a DD system is added to DD Management Center, all historical information for that system is copied to DD Management Center.

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

DD Management Center monitoring tools draw on this data for current and historical reporting and for creating trend projections.

DD Management Center 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.

DD Management Center monitoring tools help you focus on areas of interest. They can show mile-high status checks of all managed DD systems and check a specific group of DD 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 provided on monitoring pages, DD Management Center 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 DD Management Center

DD Management Center maintains up to ten years of performance and capacity measurements for the DD systems it is monitoring. Data from the DD 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, DD Management Center 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 DD Management Center retains each sample.

<table>
<thead>
<tr>
<th>type of data</th>
<th>keep hourly samples for</th>
<th>keep daily samples for</th>
<th>keep weekly samples for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection space usage</td>
<td>3 months</td>
<td>1 year</td>
<td>10 years</td>
</tr>
<tr>
<td>MTree space used</td>
<td>1 month</td>
<td>3 months</td>
<td>10 years</td>
</tr>
<tr>
<td>Automatic replication (bytes transferred and lag)</td>
<td>1 month</td>
<td>3 months</td>
<td>10 years</td>
</tr>
</tbody>
</table>
Table 1 Data retention policy for DD Management Center (continued)

<table>
<thead>
<tr>
<th>type of data</th>
<th>keep hourly samples for</th>
<th>keep daily samples for</th>
<th>keep weekly samples for</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-demand replication (number of files and bytes transferred)</td>
<td>3 months</td>
<td>1 year</td>
<td>10 years</td>
</tr>
<tr>
<td>Performance (CPU and network)</td>
<td>1 month</td>
<td>1 year</td>
<td>none created or retained</td>
</tr>
</tbody>
</table>

Finally, DD Management Center retains up to 2,000 historical alerts from each DD system being monitored.

**Space projection algorithm for DD Management Center**

DD Management Center uses a sophisticated algorithm to project growth in space usage and to predict when a DD system will run out of space. This algorithm was developed and verified using years of autosupport reports and should be quite accurate.

For this algorithm, DD Management Center 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 new 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 the fit was perfect. A value of 0 means there was no fit at all. A value of 0.8 means that DD Management Center 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. DD Management Center 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 DD system must be at least 10% full.
6. The most recent data sample must be within 5% of the projection.

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

**Performing daily monitoring**

Using DD Management Center 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 DD systems and data replication.
Checking dashboard status widgets

The Dashboard > Monitoring widgets (Current Health Status, Active Alerts, Capacity Overview, Space Usage, Replication Status, Top Replication Lags, and Replication Lag Status By Pairs) provide an overview of key performance indicators for your monitored DD systems.

You can set up from one to seven tabs to hold any combination of these widgets. 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 online, a Status button appears at the top 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 be toggled 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
The Capacity widget displays systems that are nearing warning or critical storage capacity levels.

Also, if configured, you can monitor the projected capacity usage for an upcoming selected interval.

Space Usage
The Space Usage widget lets you monitor aggregate totals of storage levels for all of the DD 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.

You can also check pre-compressed space usage and compression ratios to verify that deduplication is working as expected.

Checking replication progress

The replication widgets provide replication status, problems, and statistics.

Replication Status
The Replication Status widget highlights replications with performance problems for the widget’s monitored systems. Also, if configured, it shows the total bytes written and the total bytes replicated in the last 24 hours.

Top Replication Lags
The Top Replication Lags widget shows source DD systems with replication pairs exhibiting critical and warning lag, ranked by severity (Critical, followed by Warning) and
by longest delay. The lag time for the worst performing replication pair on the system is shown, along with the lag trend for that pair (increasing, decreasing, or holding steady). Select a system entry to open the Replication › Automatic page, showing all pairs originating from that system.

**Replication Lag Status by Pairs**
The Replication Lag Status by Pairs widget shows the count of replication pairs exhibiting Critical, Warning, and Normal threshold levels, based on the assigned policies. Selecting a bar takes you to the Replication › Automatic page, showing all pairs with that severity.

**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.

**Current Health Status**
The Current Health Status widget highlights unreachable systems and systems having problems with file system and replication operation, alerts, and data transmission protocols. The widgets show All Normal or show a count of systems exhibiting problems.

- Selecting the system count for each category navigates to the Health Status page, filtered to display the status of only that widget’s systems.
- Selecting the banner for unreachable systems navigates to the Health Status page to show the status of just the unreachable systems.
- The marker for All Normal status has no navigation or drill-down behavior.

**Active Alerts**
The Active Alerts widget displays a tally of systems with outstanding alerts for Emergency & Alert, Critical & Error, and Warning, using color-coded bar graphs.

- The length of the bar shows the total number of alerts, while color and symbol provide visual clues.
- Selecting the alert bar takes you to the Alerts page, filtered by the widget's configured filters and the type of alert category.

**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 DD Management Center 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, alerts, etc.

The Systems/Groups/Tenants icons at the top right let you show all DD systems, or DD systems organized by group or Tenant assignment.
Note
Secure Multitenancy functionality requires DD systems running DD OS 5.5 or later.

LED colors indicate:
- Red – error or problem
- Yellow – error or warning
- Green – normal operation
- Grey – disabled components
- Grey “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.

For all three views:
- Hover the cursor over a grey LED in the Replication column to get a link to the Replication Overview, showing the pairs related to this DD system or Tenant Unit.
- Hover the cursor over a red 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 in the VTL column to get a link to launch DD System Manager.
- The System Details control (top left) launches the System Details Lightbox for the selected DD system.

For the Tenants view:
- When a DD 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 (top 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 top right of the page to toggle page content to show all DD systems or DD systems organized by tenant assignment.

When you select the Tenants icon, note the following:
- The Tenant Unit Details control (top left) launches the Tenant Unit Details Lightbox.
A special “all” Tenant Unit alert is applied to all Tenant Units in the system.

**Note**

Secure Multitenancy functionality requires DD 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 top 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 shows descriptive information about the alert in the Details and the History panels, at the bottom of the page. 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 DD 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 DD system alert is selected.

**Note**

For additional information on specific alerts, see the Error Message Catalog on the EMC 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 DD Management Center, 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 Succeeded.

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

When upgrading one or more DD systems, the progress of a selected In-progress task can be paused and resumed with the Status control.

Tasks can run on the DD Management Center alone or can run on the DD Management Center and a DD system. For example, the Report Generation task runs solely on DD Management Center; other tasks, like Upgrade, run mostly on the DD system, but a skeleton process on DD Management Center keeps track of the task’s progress. And still other tasks run mostly on DD Management Center (such as Adding Systems), but have subtasks that run on the DD system. Tasks that run on DD System Manager (native to the DD system) are not shown in the Jobs list — only those tasks initiated from DD Management Center are shown.

The displayed list of tasks is dependent on the role:

- A person with a user role on a DD system or DD Management Center sees only the tasks they initiated on that DD system or DD Management Center.
An admin on a DD system or DD Management Center sees all jobs on that DD system and DD Management Center.

Monitoring capacity

The Capacity pages display information about storage utilization, allowing you to toggle between managed DD systems and MTrees. You can check current and historical space consumption, as well as estimate projected near-term future storage needs.

Checking system capacity and disk space usage

The Capacity > Utilization page displays storage usage amounts for monitored DD systems (default) or their MTrees. You can also observe disk space usage trends.

The System/MTree tabs at the top right let you choose how to display data. Then, after choosing System, there are icons (just underneath) to let you select Systems or Groups. With MTree, you can select Systems or Tenants.

In the MTree Tenants view:

- You can enter a list of comma-separated strings to filter the Tenant Unit column.
- You can also sort MTrees within a Tenant Unit.
- In the Space 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. Selecting multiple systems displays their aggregated totals.

Using this data, you can:

- 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
- Identify systems that have deviated from their norm for compression ratio, etc.
- Identify systems as targets for new back ups, replication, and migration
- View the amount of data written during a particular timeframe, such as a back-up cycle, and determine how much it has been compressed
- Identify when garbage collection runs and how much space is reclaimed
- 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

Selecting a System displays the Space Usage and Charts areas, at the bottom. For MTrees, there is also a Properties area.

In the Space Usage area, when a System is selected, space usage amounts are shown for the current time and the last 24 hours, pre-comp used, and configurable columns showing Compression Factor, Cleanable, and Capacity Thresholds for Warning and/or Critical states (by default, thresholds are set to 80% for warning and 90% for critical; they can also be set from the Inventory > Systems page Edit control). The Warning and Critical Capacity Thresholds columns can be sorted by ascending/descending controls and can also filtered by an entered value (greater, lesser, or equal to entered value).
The Space Usage amounts may not exactly match capacity totals 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.

In the Charts area, the Space Usage, Consumption, and Data Written tabs provide information about:

- Systems that are consuming space at a rate significantly greater or less than their historical norm
- Total capacity, amount 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
- 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

This guide assumes you are familiar with capacity terms, as introduced in the EMC Data Domain Operating System Administration Guide. See that guide, or the DD System Manager online help, for explanations of these terms.

**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

Each entry in the table shows the system name, model, OS version, 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, selected past, and projected months are provided. A storage graphic depicts the system’s capacity by percentage used, with color coding to show normal, warning, and critical threshold levels.

You can select the timeline to choose a specific month (past or future), which creates a date column for comparison analysis. Projections are based on historical data and require at least 15 daily data points to work.

If insufficient data prevents an accurate projection, informational messages are displayed.
Table 2 Insufficient data messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data is no longer being added to system.</td>
<td>The used capacity is basically flat, so predictions are unreliable.</td>
</tr>
<tr>
<td>Projection cannot be made.</td>
<td>The projection failed for unknown reasons.</td>
</tr>
<tr>
<td>Projection cannot be made because the average space used in the last 7 days is less than 10%.</td>
<td>The DD 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 would be unreliable.</td>
</tr>
<tr>
<td>Projection cannot be made because of insufficient data. A minimum of 15 daily space usage points is required for projections.</td>
<td>At least 15 days of data is required to make a reliable projection.</td>
</tr>
<tr>
<td>Projection cannot be made because of a large recent drop in space used.</td>
<td>A regression was computed, and the slope is negative (that is, capacity is freeing up, not being consumed).</td>
</tr>
<tr>
<td>Projection cannot be made because the space used varies too greatly during the past 15 days.</td>
<td>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.</td>
</tr>
<tr>
<td>Projection cannot be made because a specific pattern based on the most recent space usage data cannot be determined.</td>
<td>A regression was computed, but the best regression does not match the actual measurements very closely. Technically, this result indicates that the R² value (the &quot;coefficient of determination&quot;) is less than 0.8. [An R² value of 1 means a perfect fit was found. A value of 0 means no correlation was found at all.] This R² value means that capacity is not being used in a smooth, linear fashion. It is either being consumed at a varying rate or varying between being used and freed up. (See Space projection algorithm for DD Management Center on page 35 for more about R².)</td>
</tr>
<tr>
<td>Projection cannot be made because the usage trend is not consistent during the past 15 days.</td>
<td>The slope is negative (that is, capacity is freeing up, not being consumed), and the fullness date is in the past.</td>
</tr>
</tbody>
</table>

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.

The slider controls on the timeline increases or decreases the date span.

Highlighting a system in the list activates controls for examining system details and launching the DD System Manager.

Checking the System Details lightbox

The System Details lightbox provides detailed operating information about specific components of a DD system.

There is a System Details control on all of the following pages:
To activate the control, you must first select a DD system from the table. There are two tabs: Details and Charts.

The Details 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 Charts tab provides graphs that help you identify:

- whether a system's resources have been overloaded for significant time periods
- the time frames and systems to consider for a new backup or replication
- whether more systems are required

Some of the charts you can produce include:

- The **Network throughput** chart, which shows whether a DD system is experiencing bandwidth-related bottlenecks. You can determine how much network bandwidth is being used by DD systems sharing the same subnet to see if any are using more than expected or allowed by IT departments.
- The **Stream counts** chart, which shows the number of reopened read file streams in the past 30 seconds (r+), the number of active read streams (rd), the number of reopened write file streams in the past 30 seconds (w+), and the number of active write streams (wr).
- The **Protocol processing** chart, which shows the number of operations per second.
- The **Protocol throughput** chart, which shows the protocol throughput (amount of data that the file system can read from and write to the kernel socket buffer) and the wait time (time taken to send and receive 1 MB of data from the file system to the kernel socket buffer).

Charting controls allow selectable time intervals by manipulating the slider or selecting a fixed interval (1 hour, 1 day, 7 days, etc).

### Monitoring replication

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

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 application 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 will contain these addition columns: Tenant, Tenant Unit, Source Tenant, Source Tenant Unit, Destination Tenant, Destination Tenant Unit. It will 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 of 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, as well as 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 (DD system to DD 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, 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 top 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 DD 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 shown are for Pre-comp data 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 generally recoverable failures. Consequently, 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 organized by Pairs or Groups (toggle at top right).

• If the source or destination fields show an IP address instead of a host name, the DNS server configuration for the DD system must be modified. When configuring DD systems to monitor DD Boost (on-demand replication), ensure their DNS servers include configuration for both forward and reverse host name lookup. Without proper DNS server configuration, DD systems will not be able to translate from IP addresses to host names, and the source and destination paths will 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 DD 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.

Use the plus and search controls on a system's icon to show an in-depth view of all replication pairs that are configured. The minus control collapses this view.

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: Pair Details and Charts.

The Pair Details tab shows:
- the last transfer status
- the source and destination systems
- settings such as encryption and operational status
- color-coded icons showing capacity levels
- graphs for historical activity (two tabs at the bottom of the page):
  - **Pair characteristics** charts performance factors, such as pre-compression written, pre-compression replicated, post-compression replication, pre-compression remaining, network bytes and compression ratio.
  - **Lag trend** (not available for on-demand replications) charts pre-compression remaining, replication lag, pre-compression written, warning threshold, and critical threshold.

The Charts tab provides graphs for:
- pair characteristics
- CPU utilization
- data written
- network and replication throughput
- source and destination, as well as common pairs characteristics

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 DD Management Center.
- 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 host name is an IP address and cannot be matched to a registered host name.

Monitoring status with reports

Reports compile information for areas of interest on managed DD systems and for Secure Multitenancy (SMT).

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 DD Management Center, 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 DD systems:

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

There are two default report template types for Secure Multitenancy (SMT):

• 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.

Procedure

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 or Multitenancy Reports), and select Next.
4. Enter a name, and select a Template. For System, the choices are Capacity, Replication, or Status. For Multitenancy, the choices are Status or Usage. Choose one or more Sections to include, and select Next.
5. Depending on whether you selected Multitenancy or System:
   a. Multitenancy: 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.
   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.
6. Optionally, add recipient email addresses (for when the report completes and/or if an error occurs). For the Tenant Unit report template, the Tenant Unit admin emails will be added by default. For the Tenant report template, the Tenant admin email will be added by default. You can manually add or remove these emails. Select Next.

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 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.

Generating a report immediately

To generate a report immediately, select a report template 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 report, which generates an .xlsx file.

The report generation information is listed in the Report History table, where it can be viewed, renamed, or deleted.
CHAPTER 4
Managing Data Domain Systems

- Launching DD System Manager ................................................................. 50
- Upgrading DD system software ................................................................. 51
- Creating access for users ........................................................................ 52
Launching DD System Manager

From some DD Management Center pages, you can launch a DD System Manager session, for the selected DD system, to perform configuration or troubleshooting. The launched version of DD System Manager actually runs on DD Management Center – not on the DD system – thereby giving you centralized, secure, and simultaneous administration for multiple DD systems.

Note

DD Management Center 1.3 launches DD System Manager 5.6. Any new features introduced in releases later than 5.6 are not displayed or supported.

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

- Health > Alerts
- Capacity > Utilization
- Capacity > Projected
- Inventory > Systems
- Replication Pair Details lightbox
- System Details lightbox

Note

Be sure the pop-up blocker on your browser is configured to allow pop-ups for DD Management Center.

The DD System Manager session that starts (in a new window) requires no login or logout and provides complete management of the DD 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 DD system is opened).

The launched DD System Manager appears the same as a native DD System Manager session, except the navigation panel and Reports and Task Logs tabs are omitted. The banner shows the DD Management Center name, and the DD system name, OS release, and model type, as well as your management role (admin, etc.).

Note the following about launching DD System Manager from DD Management Center:

- You can launch DD System Manager only for a system for which you have an administrator role.
- A permission is comprised 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 security officer role is not supported.
- The inventory of DD systems on DD Management Center is used.
  - The DD systems shown are based on your effective permissions.
  - Only replication source and destination systems registered with DD Management Center are shown.
• You do not need to open any additional firewall ports for the session (that is, after a DD system is added to DD Management Center, the existing port assignments are used for the DD System Manager connection).

**Upgrading DD system software**

You can upgrade the DD OS on one – or a group of – DD systems, if you have admin rights on those systems and on DD Management Center.

**Procedure**
1. Get a DD OS upgrade package, by downloading an upgrade package from the EMC Online Support site.
2. Upload the DD OS upgrade package to the DD Management Center inventory.
3. Perform the DD OS upgrade on the DD system(s).

**Managing DD system upgrade packages**

Before you can upgrade a DD system through DD Management Center, you must upload the upgrade package to the DD Management Center inventory.

**Procedure**
1. Select **Inventory > Systems**.
2. Select a DD system or systems.
3. If the currently selected system(s) allow an upgrade, the banner will display **Upgrade**. In this case, select **Manage Upgrade Packages** from the drop-down list.
   
   If the currently selected system(s) do not allow an upgrade, the banner will display **Packages**. You can still select **Manage Upgrade Packages** from the drop-down list.
4. In the Manage Upgrade Packages dialog:
   - To download a package, select the EMC Online Support link, and store the package locally.
   - To upload a package to the inventory, select Add (green plus sign), and browse to the local drive to select the package. (You can also go to the EMC Online Support site through this dialog.)
   - To delete a package, select the package and then select Delete (red X).
5. After the upgrade package has been uploaded to the DD Management Center inventory, you can upgrade one or more DD systems.

**Performing a DD system upgrade**

The DD OS on one or more DD systems can be upgraded from DD Management Center with one upgrade operation.

**Procedure**
1. Select **Inventory > Systems**.
2. In the Inventory table, select one or more target systems for the DD OS upgrade.
   
   Ensure the OS column is visible.
3. From the Upgrade menu, select **Upgrade**.
4. In the Upgrade Systems dialog, select the DD OS version from the drop-down list.
Versions that display in the drop-down list reside on the DD Management Center; they have been either downloaded from the EMC Online Support site or uploaded from a local drive, as described in the previous topic.

The body of the window shows any warnings or errors. All errors must be removed before the upgrade is allowed. Errors can be removed by removing the offending system from the list, or possibly by changing the target upgrade version. You may choose to correct the condition separately, and try again later. Warnings such as those for resulting incompatible versions in a replication pair will not disallow the upgrade.

Also, if there are no packages in the DD Management Center inventory, there will be a link above the table on the right that will take the user to the **Manage Upgrade Packages** dialog.

5. Select **Upgrade** to upgrade the selected systems.

If systems are not in an acceptable managed state (for example, unreachable, suspended, upgrading) the upgrade action is unavailable.

---

**Note**

Depending on the number of DD systems selected for the upgrade and other factors, the upgrade may take a long time. After the upgrade, each DD system automatically reboots. File access is interrupted during the upgrade. Progress for the upgrade can be tracked on the **Health > Jobs** page.

---

### Creating access for users

To set up access to DD Management Center, you must add users and access groups, as well as add permissions for certain roles.

**Procedure**

1. Select **Administration > Settings > Access tab > Local Users tab**.

2. Select **Create** to add users and access groups (NIS and Active Directory) to DD Management Center.

   These users can log into DD Management Center, but cannot see any other systems. You can add permissions to view (user role), administer (admin role), or take snapshots (backup operator) for groups and DD systems.

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

3. For users and user groups with the user role, you must set permissions on DD systems so they can view the systems. Select **Administration > Permissions**.

4. Select Add (green plus sign).

5. In the Add Permissions dialog, select where to add the permission:

   - **Add permissions to systems** – Select this option, and from the list of managed DD 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.
6. In the User area, select Add (green plus sign), select one or more users from the Select Users dialog, and select Select.

7. Click in the Role field for the user, and select the access role: Administrator, Backup Operator, or User.

8. Select Add (green plus sign).

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

After you finish

To simplify the management of permissions:

- It is recommended that the use of the admin role for the DD Management Center be minimal.
  - The admin role can manage all DD systems in the DD Management Center inventory. In addition, the admin for the DD Management Center configures the DD Management Center properties and groups and assigns its permissions.
  - Configure most logins for DD Management Center 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 DD Management Center to centrally administer all systems, reducing the use of local accounts on each managed DD system. Turn off direct GUI access to DD systems that are managed by DD Management Center.

Understanding DD Management Center permissions

The Administration > Permissions pages (Assigned, Groups, Systems, Users) show the permissions of DD Management Center 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, Backup Operator, or User)

The Permissions pages are also used to add, modify, and remove permissions from groups and systems. Each of the views show the users, their assigned roles, and their effective roles.
CHAPTER 5
Administering Secure Multitenancy

- How DD Management Center helps with SMT monitoring ........................................ 56
- Creating and managing Tenants ............................................................................. 62
- Creating and managing Tenant Units ...................................................................... 65
- Creating, editing, and generating reports for SMT ..................................................... 74
How DD Management Center helps with SMT monitoring

DD Management Center can configure and monitor SMT (Secure Multitenancy) for DD Boost backup and replication storage on multiple DD systems.

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

1. The storage administrator creates Tenants on DD Management Center.
   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 DD 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 “DD Secure Multitenancy” chapter of the EMC Data Domain Operating System Administration Guide.

Data Domain Secure Multitenancy overview

Data Domain Secure Multitenancy (SMT) provides secure storage consolidation in Protection Storage.

Segregating, isolating, and protecting data of multiple customers – on a single DD system – is the main feature of SMT.

Multiple tenants can simultaneously reside on a single DD system, but the activities of one tenant cannot be detected by another.

Within an enterprise, a tenant may consist of one or more business units or departments on a DD system 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 DD 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 DD 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 DD system.

Terminology used in SMT

Understanding the terminology used in SMT (Secure Multitenancy) will help you better understand this unique environment.

**MTrees**

MTrees are logical partitions of the Data Domain 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.

**Multitenancy**

Multitenancy 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. Data Domain SMT enables *Data Protection-as-a-Service*.

**RBAC (role-based access control)**

*RBAC* (role-based access control) offers multiple roles with different privilege levels, which combine to provide the administrative isolation on a multitenant DD system. (The next section will define these roles.)

**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 DD 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* lets a Tenant log in to a DD system to access the Tenant Units assigned to him or her and perform their own administration and reporting for their own environments.

**Tenant Unit**

A *Tenant Unit* is the partition of a DD system that serves as the unit of administrative isolation between Tenants. Tenant Units 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 needed in a multitenancy setup. Users, management-groups, notification-groups, and other configuration elements are part of a Tenant Unit.

**Understanding RBAC in SMT**

In SMT (Secure Multitenancy), permission to perform a task depends on the role assigned to a user. DD Management Center uses *RBAC* (role-based access control) to control these permissions.

All DD Management Center users can:

- View all Tenants
- Create, read, update, or delete Tenant Units belonging to any Tenant if the user is an administrator on the DD system hosting the Tenant Unit
- Assign and unassign Tenant Units to and from a Tenant if the user is an administrator on the DD system hosting the Tenant Unit
- View Tenant Units belonging to any Tenant if the user has any assigned role on the DD 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 DD system. An *admin* can also perform all SMT administrative operations on a DD 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 DD Management Center *admin* and a DD OS *sysadmin* on all DD systems associated with the Tenant Units.
of that Tenant. If the Tenant does not have any Tenant Units, you need only to be a DD Management Center admin to edit or delete that Tenant.

**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. In addition, tenant-admins ensure administrative separation when Tenant self-service mode is enabled. In the context of SMT, the tenant-admin is usually 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. In addition, 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 DD 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 DD 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 DD system is logged in with the role 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 DD 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 DD Management Center and the DD system (DD OS).

**Table 3 Permission table for Tenants and Tenant Units**

<table>
<thead>
<tr>
<th>DDMC admin and DD OS sysadmin</th>
<th>DDMC admin and DD OS user/backup operator</th>
<th>DDMC user and DD OS sysadmin</th>
<th>DDMC user and DD OS user/backup operator</th>
<th>no role in DD OS</th>
<th>notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create Tenant</td>
<td>yes</td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit/delete Tenant with no Tenant Units</td>
<td>yes</td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Table 3</td>
<td>Permission table for Tenants and Tenant Units (continued)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DDMC admin</strong></td>
<td><strong>DDMC admin and DD OS sysadmin</strong></td>
<td><strong>DDMC user and DD OS user/backup operator</strong></td>
<td><strong>DDMC user and DD OS sysadmin</strong></td>
<td><strong>DDMC user and DD OS user/backup operator</strong></td>
<td><strong>no role in DD OS</strong></td>
</tr>
<tr>
<td>Edit/delete Tenant with Tenant Units</td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
<td>yes</td>
</tr>
<tr>
<td>View all Tenants defined in DDMC</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Display issue with Tenant Units for Tenant in summary page</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>View Tenant Details lightbox</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>View MTree configuration issues for Tenant in summary page</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td><strong>Tenant Unit</strong></td>
<td><strong>no role in DD OS</strong></td>
<td><strong>notes</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>See system for selection in the Create Tenant Unit Wizard</td>
<td>yes</td>
<td></td>
<td>yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit and delete Tenant Unit</td>
<td>yes</td>
<td></td>
<td>yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Tenant Units associated with DD systems listed in inventory page</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>Edit/delete unmanaged Tenant Unit</td>
<td>yes</td>
<td></td>
<td>yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign/unassign Tenant Unit to/from Tenant</td>
<td>yes</td>
<td></td>
<td>yes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 3 Permission table for Tenants and Tenant Units (continued)

<table>
<thead>
<tr>
<th></th>
<th>DDMC admin and DD OS sysadmin</th>
<th>DDMC admin and DD OS user/backup operator</th>
<th>DDMC user and DD OS sysadmin</th>
<th>DDMC user and DD OS user/backup operator</th>
<th>no role in DD OS</th>
<th>notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Tenant Unit Details lightbox</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>no role</td>
<td></td>
</tr>
</tbody>
</table>

Use cases for SMT

The following use cases summarize how SMT (Secure Multitenancy) 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-premise 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 SMT (Secure Multitenancy), 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 user name 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. Therefore, 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 DD model.)

Each backup application must authenticate using its DD Boost user name 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 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 DD Management Center. 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 DD Management Center 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 *EMC Data Domain Operating System Administration Guide*. For creating a user with the DD OS CLI, see the *EMC Data Domain Operating System Command Reference Guide*.

Using DD Management Center to administer SMT

In DD Management Center, SMT (Secure Multitenancy) is administered by selecting *Administration > Multitenancy*.

The Administration Multitenancy page shows a Tenant tree on the left, from which you can create and manage Tenants, Tenant Units, and provisioned storage.

Above this tree are controls to Add (green +), Edit (pencil), and Delete (red X) Tenants and/or Tenant Units (depending on what is highlighted in the tree), as well as a Tenant (Unit) Details (blue i) icon that displays the Tenant (Unit) Details Lightbox (again depending on what is highlighted). You can also right-click on each node in the tree to perform these functions, as well. All of these actions are controlled by RBAC (role-based access control).

Also in the tree, 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. Additionally 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 All Tenants node is always displayed and lets you create Tenant objects.

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

To the right of the tree 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.

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

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

To changed a Data Center Location, select **Administration > Properties** and edit the Data Center property. Note that each DD system must explicitly be assigned a value for Data Center in **Administration > Systems**. If a DD system has a Data Center property assigned, it will be grouped under **All/in** the Create Tenant Unit wizard.

### Storage administrator tasks in SMT

Storage administrators are the *landlords* for backup operators (*tenants*), in an SMT (Secure Multitenancy) environment. Storage administrators install and configure DD system hardware and software and use DD Management Center 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 DD systems to one or more larger systems
- Isolate each Tenant’s data from other Tenants who share storage on the same physical DD system
- Monitor and manage the space usage and performance of each system
- Monitor and manage the space usage by, and performance provided to, each Tenant, which ensures that the storage administrator meets the requirements of the service level agreement with each Tenant
- Group together 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 SMT

Backup operators are the *tenants* in an SMT (Secure Multitenancy) 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

DD Management Center provides many options for creating and managing Tenants.

### Creating Tenants

You can create Tenants from the Multitenancy page.

**Procedure**

1. Select **Administration > Multitenancy**.
2. Highlight **All Tenants** in the tree, and select Add Tenant (green plus sign) above the tree.
3. In the Create Tenant dialog, enter the following information:
   - For **Tenant name** [which is required, as indicated by the asterisk (*)], 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), enter the name of the backup administrator.
- For **Administrator email** [which is required, as indicated by the asterisk (*)], enter the email address of the backup administrator. This will be 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 Multitenancy page.

**Procedure**

1. Select **Administration** › **Multitenancy**.
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** › **Multitenancy**, 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 DD system for that Tenant Unit. Health LEDs can also be in a disabled state if the underlying component (that is, Replication, DD Boost, etc.) is either not licensed or disabled on any of the DD systems of the Tenant.
- **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), 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 used for a selected period of 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 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 period of 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 backup, 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 period of 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 DD system of a selected Tenant Unit 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 period of 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.

Procedure

1. Select Administration > Multitenancy.
2. In the tree, highlight 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.

Procedure

1. Select Administration > Multitenancy.
2. Highlight the Tenant in the tree, and select Delete Tenant (red X) above the tree.
3. In the Delete Tenant dialog, 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**.

**NOTICE**

Deleting a Tenant cannot be undone from DD Management Center, 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 DD systems under the Tenant is turned off.
- Some of the DD systems under the Tenant are not reachable or are powered down.
- The DD Boost feature of one or more of the DD systems under the Tenant is disabled or is not licensed.

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

### Creating and managing Tenant Units

DD Management Center provides many options for creating and managing Tenant Units.

#### Creating a new Tenant Unit with the wizard

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

**Before you begin**

Storage for a Tenant is contained within a virtual partition called a **Tenant Unit** on a DD 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 > Multitenancy**. 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 will be 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 will allow backup software to create Storage Units that will be assigned to this Tenant Unit.
- **Create an empty Tenant Unit**, where you can provision the Tenant Unit later using the Edit Tenant Unit dialog.
Procedure

1. On the first page of the wizard, Identify Host System:
   - For **Tenant Unit name** [which is required, as indicated with the asterisk (*)], enter a unique Tenant Unit name per system.
   - For **Administrator name** (which is optional), enter the name of the backup administrator.
   - For **Administrator email** [which is required, as indicated with the asterisk (*)], enter the email address of the backup administrator. This will be used to create a default Alert Notification list.
   - For **Datacenter location** (which is optional), enter a location. The Tenant Unit will be created only on systems at this location. This is the same Data Center location from Administration > Properties. The administrator should populate the Data Center property with values (for example, Dallas, New York, etc.). When adding a system, this property should be set for the system, depending on its location (example, Dallas). After this value has been set for any system, it will show up in the drop-down list here (Create Tenant Unit). Selecting it will then filter and show all systems based on only that Data Center location property.
   - For **Size now (GiB)** (which is optional), enter a number to filter systems that do not currently have sufficient storage capacity.
   - For **Size to grow (GiB)** (which is optional), enter 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 six months, the minimum capacity requirement would be 2 GiB.
   - For **Time to grow** (which is optional), enter 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 will see systems that have enough logical capacity to host 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 six months, the minimum capacity requirement would be 2 GiB. Any system that has a lower projected capacity will be filtered from the list. Also, any system offline at the time, as well as any collection destination system, will be filtered from the list. Also, any systems running a version prior to DD OS 5.5.x will be filtered from the list, that is, only systems running DD OS 5.5.x or later will be 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 DD system is not listed, it may be because it:
     - is not in the specified data center.
     - is offline.
     - is running DD OS 5.3 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 shows historical data, including throughput for selected connection port, CPU utilization for each system, and stream count. You can use this information to determine the best system on which to create the Tenant Unit.

3. The third page of the wizard depends on your previous choice. [Note that for “Create an empty Tenant Unit”, you will just go to the final page (step 4).]
   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 is 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 will be selected by default. If there are no local users in the list, the “New local user” will be selected. All selected users or newly created users will automatically be default Tenant Units.
      • A warning will show 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 DD Boost Data Access User dialog will change to a create new local user form.

4. The fourth (final) page (third 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) will automatically generate 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 network/connectivity issues, sudden system state changes, etc.

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 your specifications.

To see the success and/or failed information for each individual 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.

Viewing Tenant Unit information and status
You can view information about all Tenant Units from the Multitenancy page.

Procedure
1. Select Administration > Multitenancy.
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 > Multitenancy, 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, etc.) is either not licensed or disabled for the DD 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 backup, 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 DD 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.

**Procedure**

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 General tab, you can change the following:

**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.

**Procedure**

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.

Editing Tenant Units: Alert Notifications tab
Each Tenant Unit has a default alert notification list (created by the DD 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.

Procedure
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: DD Boost Data Access Users tab

DD Boost 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 DD Boost Data Access User. When your backup software creates new Storage Units for a user, the software automatically uses the default Tenant Unit.

Procedure
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 DDBoot Data Access Users tab, add, edit, or delete users, as desired. New DD Boost 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. Select OK or Apply to save your changes.
Editing Tenant Units: DDBoost 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 DD system.

Procedure

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 DDBoost 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 soft stream limits

You can configure soft 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.

Procedure

1. Select Set Limits from the DDBoost Streams tab of the Edit Tenant Unit dialog [which you can get to by selecting Administration > Multitenancy, 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, listed at right. Also note that a single value cannot be larger than the Combined limit.
3. Then, if the limits are surpassed, an alert will be generated by the DD System.
4. Select Set.

Editing Tenant Units: MTrees tab

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

Procedure

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 and/or Storage Units, as desired.

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 DD Management Center. You can adjust quotas using DD Management Center if the host system quotas have already been enabled.

Before you begin
The host system quotas must have already been enabled.

Procedure

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 MTee in the list, and select Edit (yellow pencil).

4. Set the desired quota values in the Edit MTee or Edit Storage Unit dialog, and select Save.

5. Select OK or Apply to save your changes.

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

1. Launch the DD System Manager, for the specific DD system, from DD Management Center.

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 EMC Data Domain Operating System Command Reference Guide.

Editing Tenant Units: Tenant Self-Service tab

Tenant Self-Service lets a Tenant log in to a DD system to access the Tenant Units assigned to him/her and perform his/her own administration and reporting for his/her own environment. Tenant Users and Tenant Admins will, of course, have different privileges.

Procedure

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 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.

Procedure
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 DD system on which the Tenant Unit resides is turned off.
- The DD system on which the Tenant Unit resides is not reachable or is powered down.
- The DD Boost feature of the DD 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 DD Management Center command line interfaces (you need to fix them in both places, as they are DD system-related). Then, you can try to delete the Tenant Unit again using DD Management Center.

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 DD Management Center, you cannot create an unmanaged Tenant Unit, but you can add an unmanaged Tenant Unit to a tenant.

Procedure
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.

**After you finish**

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 reports for SMT**

You can create, edit, and generate reports for SMT (Secure Multitenancy) using DD Management Center.

**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 DD Management Center and on the DD system (DD OS).

**Table 4 Permission table for Tenants and Tenant Units**

<table>
<thead>
<tr>
<th>Permission</th>
<th>DDMC admin and DD OS sysadmin</th>
<th>DDMC user and DD OS user/backup operator</th>
<th>DDMC user and DD OS sysadmin</th>
<th>DDMC user and DD OS user/backup operator</th>
<th>no role in DD OS</th>
<th>notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Report Template</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View all report templates</td>
<td>yes</td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Tenant report configuration information in summary page</td>
<td>yes</td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Tenant Unit report configuration information in summary page</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td></td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>Create Auto Tenant report template</td>
<td>yes</td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create Auto Tenant Unit report template</td>
<td>yes</td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create Manual Tenant report template</td>
<td>yes</td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**DDMC user** can view only templates or reports that they created.

Only **DDMC admin** should be allowed to create Tenant report template.

**DDMC user** is not allowed to manually create a Tenant report template.
### Table 4 Permission table for Tenants and Tenant Units (continued)

<table>
<thead>
<tr>
<th>Role</th>
<th>DDMC admin and DD OS sysadmin</th>
<th>DDMC user and DD OS user/backup operator</th>
<th>no role in DD OS</th>
<th>notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Manual Tenant Unit report template</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>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.</td>
</tr>
<tr>
<td>Maintain and tag SMT report template configuration</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
</tbody>
</table>

### Creating report templates for SMT

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

**Note**

If a user who is the “owner” of any report templates is deleted from DD Management Center, those report templates will still appear to be owned by the “deleted” user, but the reports will no longer run at their scheduled times.

**Procedure**

1. Select **Reports > Management**.
2. Select **Add** (green plus sign).
3. In the Add Report Template dialog, select **Multitenancy Reports** and select **Next**.
4. Enter 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 will be two hours ahead of **Starts On** time.
6. For the Tenant Unit report template, the Tenant Unit admin emails will be added by default. For the Tenant report template, the Tenant admin email will be added by default. You can manually add or remove these emails.
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 multitenancy 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 report templates

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

Procedure
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 time 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.

Generating reports

A report can be generated after the last step of the create report wizard or, as described below, by selecting a report template listed in the Template name table, and selecting Run Report.

Procedure
1. Select Reports › Management.
2. Select a report template from the list.
3. Right-click on the name, and select Run Report.

Results
A report (named by concatenating the datestamp to the template title) is created and opened as a PDF file in your 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.
CHAPTER 6
Performing Additional Configuration

- Managing access to DD Management Center ............................................................. 78
- Viewing active users ............................................................................................... 93
- Managing network settings ................................................................................... 93
- Upgrading DD Management Center software ......................................................... 104
- Checking a DD Management Center serial number ................................................. 105
- Managing alerts .................................................................................................... 105
- Managing general configuration settings ............................................................... 108
- Managing autosupport reporting .......................................................................... 115
- Managing system logs .......................................................................................... 116
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 DD Management Center tasks

Since mutual trust is established between DD Management Center and its managed DD systems, if a user is added to DD Management Center with admin level access, that user can also access the managed DD systems (through ssh or by launching DD System Manager) to perform admin-level operations. Also, an admin-level user can upgrade a managed DD system. Therefore, you should give each new DD Management Center user the same consideration that you would a new DD System Manager user.

The roles available in DD Management Center are the same as those in DD System Manager:

- **admin**, that is, the *DD Management Center Administrator*. An admin can access all functions on a DD Management Center page.
- **user**, that is, a *DD Management Center User*. A user, which can be a stand-alone user or part of a group, has access to only certain functions on a DD Management Center page, based on the role assigned to that user or group.

The following table shows the actions available for each feature of DD Management Center. [This table is mainly provided to show when only the *user* role is required. The *admin* role can perform all tasks, as previously mentioned.]

<table>
<thead>
<tr>
<th>action</th>
<th>minimum permission</th>
<th>description of actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage permissions</td>
<td>DD Management Center Administrator</td>
<td>Assign, edit, remove permissions for users</td>
</tr>
<tr>
<td>Manage DD systems</td>
<td>DD Management Center Administrator</td>
<td>Add, edit, delete systems from the inventory</td>
</tr>
<tr>
<td>Manage users / user groups</td>
<td>DD Management Center Administrator</td>
<td>Add, edit, delete local users and AD/NIS user groups</td>
</tr>
<tr>
<td>Configure DD Management Center</td>
<td>DD Management Center Administrator</td>
<td>Work with DD Management Center Administration &gt; Settings pages</td>
</tr>
<tr>
<td>Upgrade DD systems</td>
<td>DD Management Center User/Administrator on the system to upgrade</td>
<td>Run the DD System Upgrade function</td>
</tr>
<tr>
<td>Upgrade DD Management Center</td>
<td>DD Management Center Administrator</td>
<td>Run the DD Management Center Upgrade function</td>
</tr>
<tr>
<td>Manage groups</td>
<td>DD Management Center Administrator</td>
<td>Create, edit, delete groups</td>
</tr>
<tr>
<td>Manage properties</td>
<td>DD Management Center Administrator</td>
<td>Create, edit, delete properties</td>
</tr>
<tr>
<td>Assign properties</td>
<td>DD Management Center Administrator</td>
<td>Assign properties to DD systems</td>
</tr>
</tbody>
</table>
Table 5 Roles required for DD Management Center tasks (continued)

<table>
<thead>
<tr>
<th>action</th>
<th>minimum permission</th>
<th>description of actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign to groups</td>
<td>DD Management Center</td>
<td>Assign DD systems to groups</td>
</tr>
<tr>
<td>Manage reports</td>
<td>DD Management Center</td>
<td>Create report templates and schedule report creation</td>
</tr>
<tr>
<td>Manage dashboard widgets</td>
<td>DD Management Center</td>
<td>Create dashboard widgets</td>
</tr>
<tr>
<td>Configure dashboard</td>
<td>DD Management Center</td>
<td>Configure widgets and dashboard layouts</td>
</tr>
<tr>
<td>Manage global filter rules</td>
<td>DD Management Center User</td>
<td>Add, edit, delete filter rules</td>
</tr>
<tr>
<td>Launch DD System Manager</td>
<td>DD Management Center User</td>
<td>Launch the virtual DD System Manager [note that Administrator privilege is required on the managed DD system to change anything]</td>
</tr>
<tr>
<td>Manage user jobs</td>
<td>DD Management Center User</td>
<td>Suspend, resume, cancel jobs owned by user</td>
</tr>
<tr>
<td>Manage all jobs</td>
<td>DD Management Center</td>
<td>Suspend, resume, cancel any job</td>
</tr>
<tr>
<td>Manage advanced replication</td>
<td>DD Management Center</td>
<td>View replication status, export to CVS file, assign properties</td>
</tr>
<tr>
<td>Manage basic replication</td>
<td>DD Management Center User</td>
<td>View replication status, export to CVS file</td>
</tr>
</tbody>
</table>

Managing administrator access

Administrator Access provides settings to configure how users can connect to DD Management Center. Each protocol is configured separately, using the procedures in this section.

Procedure

1. Select **Administration > Settings > Access tab > Administrator Access tab**.
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 *EMC Data Domain Operating System Administration Guide*.) You can also view the available services, and for a selected service, the service options that are configured for it.

Table 6 Services

<table>
<thead>
<tr>
<th>item</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 6 Services (continued)

<table>
<thead>
<tr>
<th>item</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Status of the service: either enabled or disabled.</td>
</tr>
<tr>
<td>Allowed Hosts</td>
<td>Access permissions set for the named host.</td>
</tr>
</tbody>
</table>

Table 7 Service options

<table>
<thead>
<tr>
<th>service name</th>
<th>option name</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>Session Timeout</td>
<td>Configured number of elapsed seconds before the service times out, or Infinite.</td>
</tr>
<tr>
<td>FTPS</td>
<td>Session Timeout</td>
<td>Configured number of elapsed seconds before the service times out, or Infinite.</td>
</tr>
<tr>
<td>HTTP/HTTPS</td>
<td>HTTP/HTTPS port</td>
<td>If applicable, port number opened for the HTTP/HTTPS protocol (HTTP – port 80, by default; HTTPS – port 443, by default).</td>
</tr>
<tr>
<td></td>
<td>Session Timeout</td>
<td>Configured number of elapsed seconds before the service times out, or Infinite.</td>
</tr>
<tr>
<td>SCP/SSH</td>
<td>SCP/SSH port</td>
<td>If applicable, port number opened for the SCP/SSH protocol (port 22, by default).</td>
</tr>
<tr>
<td></td>
<td>Session Timeout</td>
<td>Configured number of elapsed seconds before the service times out, or Infinite.</td>
</tr>
<tr>
<td>Telnet</td>
<td>Session Timeout</td>
<td>Configured number of elapsed seconds before the service times out, or Infinite.</td>
</tr>
</tbody>
</table>

Managing FTP access

You can provide access to DD Management Center through an FTP connection.

Procedure
1. Select Administration > Settings > Access tab > Administrator Access tab.
2. In the Services are, select the checkbox next to FTP, and select Configure.
3. In the Configure FTP Access dialog, select Allow FTP Access. If FTPS is enabled, it will be disabled before enabling FTP.
4. Determine how hosts are to connect:
   - Allow all hosts to connect
   - Limit access to the following systems – Then, select the appropriate icon under Allowed 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 select OK.
     - To modify a host name, select the checkbox next to the host name in the Hosts list, select Edit (pencil), change the host name, and select OK.
     - To remove a host name, select the checkbox next to the host name in the Hosts list, select Delete (X), and select OK.
5. To configure a session timeout value, select the **Advanced** tab.

6. In **Session Timeout**, enter, 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.

7. Select **OK**.

### Managing FTPS access

You can provide access to DD Management Center through an FTPS connection.

**Procedure**

1. Select **Administration** > **Settings** > **Access tab** > **Administrator Access tab**.
2. In the Services panel, select the checkbox next to FTPS, and select **Configure**.
3. In the Configure FTPS Access dialog, select **Allow FTPS Access**. If FTP is enabled, it will be disabled before FTPS is enabled.
4. Determine how hosts are to connect:
   - **Allow all hosts to connect**
   - **Limit access to the following systems** – Then, select the appropriate icon under **Allowed 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 select **OK**.
     - To modify a host name, select the checkbox next to the host name in the **Hosts** list, select Edit (pencil), change the host name, and select **OK**.
     - To remove a host name, select the checkbox next to the host name in the **Hosts** list, select Delete (X), and select **OK**.

5. To configure a session timeout value, select the **Advanced** tab.

6. In **Session Timeout**, enter, 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.

7. Select **OK**.

### Managing HTTP/HTTPS access

You can provide access to DD Management Center through an HTTP and/or HTTPS connection.

**Procedure**

1. Select **Administration** > **Settings** > **Access tab** > **Administrator Access tab**.
2. In the **Services** area, select the checkbox next to **HTTP** or **HTTPS**, and select **Configure**.
3. In the Configure HTTP/HTTPS Access dialog, select the checkbox for **Allow HTTP Access** and/or **Allow HTTPS Access**.
4. Determine how hosts are to connect:
   - **Allow all hosts to connect**
   - **Limit access to the following systems** – Then, select the appropriate icon under **Allowed 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 select **OK**.
     - To modify a host name, select the checkbox next to the host name in the **Hosts** list, select Edit (pencil), change the host name, and select **OK**.
To remove a host name, select the checkbox next to the host name in the Hosts list, select Delete (X), and select OK.

5. To configure system ports and session timeout values, select the Advanced tab.
   - For HTTP Port, enter the port for connection. Port 80 is assigned by default.
   - For HTTPS Port, enter the port for connection. Port 443 is assigned by default.
   - For Session Timeout, enter, in seconds, the interval that must elapse before the connection closes. 10800 seconds (3 hours) is assigned by default.

---

**Note**

Select Default to return a setting back to its default value.

6. Select OK.

**Managing SCP/SSH access**

You can provide access to DD Management Center through an SCP and/or SSH connection.

**Procedure**

1. Select Administration > Settings > Access tab > Administrator Access tab.
2. In the Services area, select the checkbox next to SCP or SSH, and select Configure.
3. In the Configure SSH/SCP Access dialog, select options to allow SSH or SCP (or both) access. SCP cannot be enabled unless SSH is enabled, as well.
4. Determine how hosts are to connect:
   - **Allow all hosts to connect**
   - **Limit access to the following systems** – Then, select the appropriate icon under Allowed 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 select OK.
     - To modify a host name, select the checkbox next to the host name in the Hosts list, select Edit (pencil), change the host name, and select OK.
     - To remove a host name, select the checkbox next to the host name in the Hosts list, select Delete (X), and select OK.

5. To configure a session timeout value, select the Advanced tab.
6. In SSH/SCP Port, enter the port number. In Session Timeout, enter, 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.
7. Select OK.

**Managing Telnet access**

You can provide access to DD Management Center through a Telnet connection.

**Procedure**

1. Select Administration > Settings > Access tab > Administrator Access tab.
2. In the Services area, select the checkbox next to Telnet, and select Configure.
3. In the Configure Telnet Access dialog, select the Allow Telnet Access checkbox.
4. Determine how hosts are to connect:
   - Allow all hosts to connect
   - Limit access to the following systems – Then, select the appropriate icon under Allowed 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 select OK.
     - To modify a host name, select the checkbox next to the host name in the Hosts list, select Edit (pencil), change the host name, and select OK.
     - To remove a host name, select the checkbox next to the host name in the Hosts list, select Delete (X), and select OK.

5. To configure a session timeout value, select the Advanced tab.

6. In Session Timeout, enter, 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.

7. Select OK.

Managing local user access to DD Management Center

The extent to which you can manage local user access to DD Management Center depends on your role.

If you are an administrator on DD Management Center, you become a global administrator, and you can configure and monitor all managed DD systems.

If you are a user on DD Management Center, you can view only the managed DD systems to which you have been assigned a user or admin role by a DD Management Center administrator.

Viewing local user information

The datestamps 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.

Procedure

1. Select Administration > Settings > Access tab > Local Users tab.

2. On the Local Users page, view information for the configured users.

<table>
<thead>
<tr>
<th>Item</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>User ID, as added to the system.</td>
</tr>
<tr>
<td>Management Role</td>
<td>Possible roles of users based on a set of privileges:</td>
</tr>
<tr>
<td></td>
<td>• admin role: Can configure and monitor the entire DD system.</td>
</tr>
<tr>
<td></td>
<td>• user role: Can monitor DD systems and perform the fastcopy operation.</td>
</tr>
<tr>
<td></td>
<td>Users with admin roles can view all users. Users with user roles can view</td>
</tr>
<tr>
<td></td>
<td>only their own user account.</td>
</tr>
<tr>
<td>Status</td>
<td>• enabled – User access to the account is permitted.</td>
</tr>
<tr>
<td></td>
<td>• disabled – User access to the account is denied because the expiration</td>
</tr>
<tr>
<td></td>
<td>date for the account has been reached or a locked</td>
</tr>
</tbody>
</table>
3. Select a specific user to see Detailed Information.

<table>
<thead>
<tr>
<th>item</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Last Changed</td>
<td>Date the password was last changed.</td>
</tr>
<tr>
<td>Minimum Days Between Change</td>
<td>Minimum number of days between password changes that you allow a user. Default is 0.</td>
</tr>
<tr>
<td>Maximum Days Between Change</td>
<td>Maximum number of days between password changes that you allow a user. Default is 90.</td>
</tr>
<tr>
<td>Warn Days Before Expire</td>
<td>Number of days to warn the users before their password expires. Default is 7.</td>
</tr>
<tr>
<td>Disable Days After Expire</td>
<td>Number of days after a password expires to disable the user account. Default is never.</td>
</tr>
</tbody>
</table>

**Note**

The default password policy can be changed by an admin by selecting **More Tasks > Change Login Options**. Default values are the initial default password policy values.

**User roles**

Roles provide a way to restrict user access to system functions by using a set of privileges. Permissions allow an admin access to specific groups and systems, reducing the need to configure every user as a global admin.

DD Management Center supports the following roles:

- **admin role**: This role can configure and monitor the entire DD Management Center system.

  **Note**

  It is recommended that the admin role be used judiciously and awarded to very few users, as these users will be able to configure DD Management Center as well as have access to all registered DD systems.

- **user role**: This role can monitor DD Management Center and DD systems for which the user has permission.
Creating local users

You can create new users with either the admin or the user role.

Procedure

1. Select Administration > Settings > Access tab > Local Users tab.
2. Select Create.
3. In the Create User dialog, enter the following in the General tab:

<table>
<thead>
<tr>
<th>item</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>User ID or name.</td>
</tr>
<tr>
<td>Password</td>
<td>User password. Set a default password, and the user can change it later.</td>
</tr>
<tr>
<td></td>
<td>The default value for the minimum length of a password or minimum number of</td>
</tr>
<tr>
<td></td>
<td>character classes required for a user password is 1.</td>
</tr>
<tr>
<td></td>
<td>Allowable character classes include:</td>
</tr>
<tr>
<td></td>
<td>• lowercase letters (a-z)</td>
</tr>
<tr>
<td></td>
<td>• uppercase letters (A-Z)</td>
</tr>
<tr>
<td></td>
<td>• numbers (0-9)</td>
</tr>
<tr>
<td></td>
<td>• special characters ($, %, #, +, and so on)</td>
</tr>
<tr>
<td>Verify Password</td>
<td>User password, again.</td>
</tr>
<tr>
<td>Management Role</td>
<td>Management role assigned to the user:</td>
</tr>
<tr>
<td></td>
<td>• admin role: Can configure and monitor the entire DD Management Center and</td>
</tr>
<tr>
<td></td>
<td>all DD systems.</td>
</tr>
<tr>
<td></td>
<td>• user role: Can monitor DD Management Center and DD systems for which they</td>
</tr>
<tr>
<td></td>
<td>have permission.</td>
</tr>
</tbody>
</table>

4. Enter the following in the Advanced tab:
### Table 9 Advanced tab

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Days Between Change</td>
<td>Minimum number of days between password changes that you allow a user. Default is 0.</td>
</tr>
<tr>
<td>Maximum Days Between Change</td>
<td>Maximum number of days between password changes that you allow a user. Default is 99999.</td>
</tr>
<tr>
<td>Warn Days Before Expire</td>
<td>Number of days to warn the users before their password expires. Default is 7.</td>
</tr>
<tr>
<td>Disable Days After Expire</td>
<td>Number of days after a password expires to disable the user account. Default is Never.</td>
</tr>
<tr>
<td>Disable account on the following date</td>
<td>Check this box and enter a date (mm/dd/yyyy) when you want to disable this account. Also, you can click the calendar to select a date. This date uses GMT.</td>
</tr>
</tbody>
</table>

5. Select **OK**.

**Note**

The default password policy can be changed by the admin using **More Tasks > Change Login Options**. The default values are the initial default password policy values.

### Modifying a local user profile

You can modify several aspects of a local user profile.

**Procedure**

1. Select **Administration > Settings > Access tab > Local Users tab**.
2. Select a user name, and select **Modify**.
3. In the Modify User dialog, change the assigned role.
4. Enter the following information in the Advanced tab:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Days Between Change</td>
<td>Minimum number of days between password changes that you allow a user. Default is 0.</td>
</tr>
<tr>
<td>Maximum Days Between Change</td>
<td>Maximum number of days between password changes that you allow a user. Default is 99999.</td>
</tr>
<tr>
<td>Warn Days Before Expire</td>
<td>Number of days to warn the users before their password expires. Default is 7.</td>
</tr>
<tr>
<td>Disable Days After Expire</td>
<td>Number of days after a password expires to disable the user account. Default is Never.</td>
</tr>
</tbody>
</table>

5. Optionally, configure a disable date (which uses GMT) for the user account.
6. Select **OK**.
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.

Procedure
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, select OK and Close.

Enabling or disabling local users

You can enable or disable local users.

Procedure
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, select OK and Close.

Changing user passwords

The Change Password dialog lets you change the password for a selected user.

Procedure
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. Select OK.

Changing login options

You can modify settings for password composition, time to change passwords, limiting login attempts, etc.

Procedure
1. Select Administration > Settings > Access tab > Local Users tab > More Tasks > Change Login Options
2. In the Change Login Options dialog, enter the password policy information. To select the default value, select the Default button next to each value.

<table>
<thead>
<tr>
<th>item</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Days Between Change</td>
<td>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.</td>
</tr>
<tr>
<td>Maximum Days Between Change</td>
<td>Maximum number of days between password changes. Default is 90.</td>
</tr>
<tr>
<td>Warn Days Before Expire</td>
<td>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.</td>
</tr>
</tbody>
</table>
### item | description
--- | ---
**Disable Days After Expire** | Number of days after a password expires to disable a user account. You may enter never or a number greater than 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:
- lowercase letters (a-z)
- uppercase letters (A-Z)
- numbers (0-9)
- special characters ($, %, #, +, etc.)

**Lowercase Character Requirement** | Enable or disable the requirement for a least one lowercase character. Default is disabled.

**Uppercase Character Requirement** | Enable or disable the requirement for a least one uppercase character. Default is disabled.

**One Digit Requirement** | Enable or disable the requirement for a least one numerical character. Default is disabled.

**Special Character Requirement** | 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.

**Prevent use of Last N Passwords** | Specify the number of remembered passwords. The range is 0 to 24. Default is 1.

**Maximum login attempts** | Specify the maximum number of login attempts 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 attempts. When the configured unlock timeout is reached, a user can re-attempt to login. The range is 120 to 3600 seconds. Default is 120.

3. Select **OK**.

### Configuring authentication

DD Management Center lets you configure three types of authentication: Active Directory/Kerberos, Workgroup, and NIS.

**Active Directory/Kerberos authentication**

If Active Directory is configured, you can use the Active Directory/Kerberos Authentication panel to view associated information.

**Procedure**

1. Select **Administration > Settings > Access tab > Authentication tab.**
2. In the Active Directory/Kerberos Authentication area, view information about Windows/Active Directories, as described in the following table.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Type of authentication mode (Disabled, or Windows/Active Directory)</td>
</tr>
<tr>
<td>Realm</td>
<td>Realm name of the Windows/Active Directory</td>
</tr>
<tr>
<td>DDNS Windows Mode</td>
<td>Whether DDNS Windows Mode is enabled or disabled</td>
</tr>
<tr>
<td>Domain Controllers</td>
<td>Name of domain controller for Windows/Active Directory</td>
</tr>
<tr>
<td>Organizational Unit</td>
<td>Name of organizational unit for Windows/Active Directory</td>
</tr>
<tr>
<td>CIFS Server Name</td>
<td>Name of the CIFS server in use</td>
</tr>
<tr>
<td>WINS Server</td>
<td>Name of the WINS server in use</td>
</tr>
<tr>
<td>Short Domain Name</td>
<td>Abbreviated name for the domain</td>
</tr>
</tbody>
</table>

3. You may configure any of this information by selecting Configure.

**Configuring Active Directory/Kerberos authentication**

DD Management Center must meet all Active Directory requirements, such as a clock time that differs no more than five minutes from that of the domain controller.

**Procedure**

1. Select Administration > Settings > Access tab > Authentication tab.
2. In the Active Directory/Kerberos Authentication area, select Configure.
3. Choose one of the following:
   - **Disabled**: NFS clients will not use Kerberos authentication. CIFS clients will use Workgroup authentication.
   - **Windows/Active Directory**: NFS clients and CIFS clients will use Kerberos authentication.

**Entering Realm Name and credentials**

A Windows KDC (Key Distribution Center) requires the Realm Name and credentials for Active Directory authentication.

**Procedure**

1. In the Realm Name text box, enter the complete realm name for DD Management Center, 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 Kerberos settings

You may optionally configure advanced Kerberos settings for CIFS Server Name, Domain Controllers, and Organizational Unit.

Procedure

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.

After you finish

After configuring Windows authentication, you must enable CIFS authentication from the DD Management Center 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.

Procedure

1. Select Administration > Settings > Access tab > Authentication tab.
2. In the Active Directory/Kerberos Authentication area, select Create to display the Create Windows Group dialog.
3. Enter the group name in the text box. The domain for the group must be specified. For example, domain\group name.
4. Select either admin or user from the Management Role drop-down list.
5. Select OK.

Modifying Windows groups

After you have created a Windows group, you can modify it, as needed.

Procedure

1. Select Administration > Settings > Access tab > Authentication tab.
2. In the Active Directory/Kerberos Authentication area, choose a Windows group from the list, and select **Modify** to display the Modify Windows Group dialog.

3. Edit the group name in the text box. The domain for the group must be specified, for example, domain\group name.

4. Select either admin or user from the Management Role drop-down list.

5. Select **OK**.

### 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.

**Procedure**

1. Select **Administration > Settings > Access tab > Authentication tab**.

2. In the **Active Directory/Kerberos Authentication** area, choose a Windows group from the list, and select **Delete** to display the Delete Windows Group dialog.

3. Select **OK**.

### Configuring Workgroup authentication

Workgroup mode joins DD Management Center to a workgroup domain.

**Procedure**

1. Select **Administration > Settings > Access tab > Authentication tab**.

2. In the Workgroup Authentication area, select **Configure** to display the Workgroup Authentication dialog.

3. For Workgroup Name, select **Manual** to enter a different Workgroup name in the text box.

4. For CIFS Server Name, select **Manual** to enter a different CIFS server name (DD system) in the text box.

5. Select **OK**.

### NIS authentication

Local user accounts on a DD system start with a UID of 500. When you set up a DD system 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.

**Procedure**

1. Select **Administration > Settings > Access tab > Authentication tab**.

2. In the NIS Authentication area, view information about NIS Servers and configured NIS Groups, as described in the following table.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIS Status</td>
<td>Status of service: enabled or disabled</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Name of domain for this service</td>
</tr>
<tr>
<td>Server</td>
<td>Name of server performing authentication</td>
</tr>
</tbody>
</table>
Table 12 NIS Authentication Information (continued)

<table>
<thead>
<tr>
<th>item</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIS Group</td>
<td>Name of NIS group</td>
</tr>
<tr>
<td>Management Role</td>
<td>Management role assigned to group (admin or user)</td>
</tr>
</tbody>
</table>

3. 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.

**Procedure**

1. Select Administration › Settings › Access tab › Authentication tab.
2. In the NIS Authentication area, next to NIS Status, select Enable to display the Enable NIS dialog.
3. Select OK.

**Disabling NIS authentication**

After you have enabled NIS authentication, you may occasionally need to disable it.

**Procedure**

1. Select Administration › Settings › Access tab › Authentication tab.
2. In the NIS Authentication area, next to NIS Status, select Disable to display the Disable NIS dialog.
3. Select OK.

**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.

**Procedure**

1. Select Administration › Settings › Access tab › Authentication tab.
2. In the NIS Authentication area, next to the Domain Name, select Edit to display the Configure NIS Domain Name dialog.
3. Enter the new domain name in the Domain Name text box.
4. Select OK.

**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.

**Procedure**

1. Select Administration › Settings › Access tab › Authentication tab.
2. In the NIS Authentication area, select Manually Configure, immediately above the Server area, if it is not selected.
3. To add a server, select Add (green plus sign) to display the Add Authentication Server dialog. Enter a name, and select OK.

4. To modify a server, select the server and Modify (yellow pencil) to display the Modify Authentication Server dialog. Edit the name, and select OK.

5. To delete a server, select the server, then Delete (red X), and then OK.

**Configuring NIS groups**
You can add, modify, or delete NIS groups.

**Procedure**
1. Select Administration > Settings > Access tab > Authentication tab.
2. In the NIS Authentication area, use the icons immediately above the NIS Group area.
3. To add a group, select Add (green plus sign) to display the Add NIS Group dialog. Enter a name, select a management role (admin or user), select Validate, and select OK.
4. To modify a group, select the group and Modify (pencil) to display the Modify NIS Group dialog. Edit the name and/or management role (admin or user), select Validate, and select OK.
5. To delete a group, select the group, Delete (X), and OK.

**Viewing active users**
You can view a variety of information about users who are currently logged in to DD Management Center.

1. Select Administration > Settings > Active Users tab.
2. View the list of active users displayed.

**Table 13 Active users**

<table>
<thead>
<tr>
<th>item</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of user with an active session</td>
</tr>
<tr>
<td>Idle</td>
<td>Amount of time since last activity for user</td>
</tr>
<tr>
<td>Last Login From</td>
<td>System where user is logged in</td>
</tr>
<tr>
<td>Last Login Time</td>
<td>Datestamp when user logged in</td>
</tr>
<tr>
<td>Tty</td>
<td>Terminal notation for CLI login or GUI if user is logged in using the GUI</td>
</tr>
</tbody>
</table>

**Managing network settings**
The Administration > Settings > Network page presents status and configuration information for network interfaces, settings, and routes, accessible by tabs. By default,
the Interfaces tab initially displays. Use this area to configure networking for the DD Management Center.

Configuring network interfaces

You can configure physical network connections and create VLANs and IP aliases for DD Management Center.

Viewing interface information

The Interfaces page (Administration > Settings > Network tab > Interfaces 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 Interface Details area.

Table 14 Interfaces area

<table>
<thead>
<tr>
<th>item</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of each Ethernet interface associated with DD Management Center.</td>
</tr>
<tr>
<td></td>
<td>Physical interfaces names start with eth.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Lets you view or change status of the interface.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Yes</strong> to enable interface and connect it to the network.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>No</strong> to disable interface and disconnect it from the network.</td>
</tr>
<tr>
<td>DHCP</td>
<td>Indicates whether the interface is configured with an IP address from a DHCP</td>
</tr>
<tr>
<td></td>
<td>(Dynamic Host Configuration Protocol) server.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address associated with the interface, which is used by the network to</td>
</tr>
<tr>
<td></td>
<td>identify the interface. If the interface is configured through DHCP, an asterisk</td>
</tr>
<tr>
<td></td>
<td>appears after this value.</td>
</tr>
<tr>
<td>Netmask</td>
<td>Netmask associated with the interface. Uses the standard IP network mask</td>
</tr>
<tr>
<td></td>
<td>format. If the interface is configured through DHCP, an asterisk appears after</td>
</tr>
<tr>
<td></td>
<td>this value.</td>
</tr>
<tr>
<td>Link</td>
<td>Indicates whether the interface currently has a live Ethernet connection.</td>
</tr>
<tr>
<td>Additional Info</td>
<td>Provides additional settings for the interface, for example, the bonding mode.</td>
</tr>
</tbody>
</table>

To populate the Interface Details area, select an interface.

Table 15 Interface Details area

<table>
<thead>
<tr>
<th>item</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>Name of selected interface.</td>
</tr>
<tr>
<td>Hardware Address</td>
<td>MAC address of selected interface, for example,</td>
</tr>
<tr>
<td></td>
<td>00:02:b3:b0:8a:d2</td>
</tr>
<tr>
<td>Cable</td>
<td>Indicates whether interface is Copper.</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transfer Unit value assigned to interface.</td>
</tr>
</tbody>
</table>
### Table 15 Interface Details area (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Negotiate</td>
<td>Indicates whether interface is enabled to automatically negotiate Speed and Duplex settings. If it is disabled, then Speed and Duplex values are manually set.</td>
</tr>
<tr>
<td>Duplex</td>
<td>Protocol used with Speed value, which sets data transfer protocol. Values are Unknown, Full, or Half.</td>
</tr>
<tr>
<td>Speed</td>
<td>Protocol 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.</td>
</tr>
<tr>
<td>Supported Speeds</td>
<td>Lists all speeds the interface is capable of using.</td>
</tr>
</tbody>
</table>

### Filtering the interfaces table

You can filter the interfaces table by All, VLAN, or IP Aliases interfaces.

**Procedure**

1. Enter a value in the Interface Name field, or select a value from the Interface Type menu. The value All displays physical, VLAN, and IP Alias interfaces.
2. Select **Update**.
3. To return the interfaces table to the default listing, select **Reset**.

### Configuring physical interfaces

You can configure physical interfaces, specifying how the interface IP address is to be set, specifying speed/duplex settings, and more.

**Procedure**

1. On the Interfaces page, select an interface to configure from the Interface list, and select **Configure**.
2. In the Configure Interface dialog, decide how the interface IP address is to be set:
   - **Obtain IP Address using DHCP**
     Setting a physical interface to DHCP automatically enables the interface.
   - **Manually configure IP Address**
     The IP Address and Netmask fields become active.
     - Enter an IP Address.
     - Enter a Netmask address.
     The format is typically 255.255.255.000. If you do not specify a netmask, DD Management Center uses the netmask format determined by your TCP/IP address class (A,B,C).
   The combination of speed and duplex settings defines the rate of data transfer through the interface. Select one of these options:
   - **Autonegotiate Speed/Duplex**
     The network interface card will autonegotiate the line speed and duplex setting for an interface. Optical interfaces require the autonegotiate option.
- **Manually configure Speed/Duplex**
  - The Speed and Duplex fields become active.
    - Select a speed, which is limited to the capabilities of the hardware device.
    - Select half-duplex or full-duplex or unknown.

4. Specify the MTU (Maximum Transfer Unit) size for the physical (Ethernet) interface.
   - Supported values are from 350 to 9014. Ensure that all of your network components support the size set with this option. The default is 1500 (and the Default button will return it to that value).

5. Select Next.

6. In the summary, confirm that the values listed reflect the new system and interface state, and if so, select Finish and OK. If not, select Back and redo your settings.

### Configuring a VLAN

You can create a new VLAN interface from a physical interface. The recommended total number of VLAN interfaces that can be created is 80. However, it is possible to create up to 100 interfaces (minus the number of aliases and physical interfaces) before the system prevents any more from being created.

**Procedure**

1. On the Interfaces tab (Administration > Settings > Network), from the Create menu, select the VLAN option.
2. In the Create VLAN dialog, specify a VLAN Id. The range of a VLAN ID is between 1 and 4094 inclusive.
3. Enter an IP Address.
4. Enter a Netmask address.
   - If you do not specify a netmask, the DD system uses the netmask format determined by your TCP/IP address class (A,B,C).
5. Specify MTU Settings, which set the Maximum Transfer Unit size for the physical (Ethernet) interface. Supported values are from 350 to 9014. For 100 Base-T and gigabit networks, 1500 is the standard default. Make sure that all of your network components support the size set with this option. The Default button returns the setting to the default value.

   **NOTICE**
   
   Incorrect MTU size can affect the system’s network performance.

6. Select Next to see a summary of your new values.
7. On the summary page, review the new values, and select Back if you want to change any of these values.
8. When you are done, select Finish and OK.

### Modifying a VLAN interface

You can modify the settings on an existing VLAN interface.

**Procedure**

1. Select the checkbox of the interface, and disable the VLAN interface by selecting No in the Enabled column. Then, select OK in the warning dialog.
2. Again select the checkbox of the (now disabled) interface, and select the Configure button.
3. In the Configure VLAN Interface dialog, change any settings.
4. Select Next and Finish.

Creating an IP Alias interface

You can create a new IP Alias interface from a physical or VLAN interface. It is recommended that the total number of IP Alias, VLAN, and physical interfaces not exceed 80, although it is possible to have up to 100.

Procedure
1. Select an interface, and choose the IP Alias option from the Create drop-down menu.
2. In the Create IP Alias dialog, enter a number for the IP Alias ID.
   This number can be from 1 to 4094, inclusive.
3. Enter an IP Address.
4. Enter a Netmask address.
   The format is typically 255.255.255.000. If you do not specify a netmask, the format is determined by the TCP/IP address class (A,B,C) in use.
5. Specify the Dynamic DNS Registration option. (This option is available only if DDNS has been registered.)
   Dynamic DNS (DDNS) is the protocol that allows machines on a network to communicate with, and register their IP address on, a Domain Name System (DNS) server.
6. Select Next.
7. Review the summary of your changes, and select Back to adjust anything, or select Finish and OK.

Modifying an IP Alias interface

You can modify the settings on an existing IP Alias interface.

Procedure
1. Select the checkbox of the interface, and disable the IP Alias interface by selecting No in the Enabled column. Then, select OK in the warning dialog.
2. Again select the checkbox of the (now disabled) interface, and select the Configure button.
3. In the Configure IP Alias dialog, change any settings.
4. Select Next and Finish.

Destroying an interface

Destroying an interface applies to VLAN and IP Alias interfaces. Destroying a VLAN deletes the VLAN and all IP Alias interfaces that are created under it, if any. Destroying an IP Alias deletes only that alias interface.

Procedure
1. In the Interfaces list, select the box next to the interface to destroy (VLAN or IP Alias).
2. Select Destroy.
3. In the Confirm Destroy dialog, select **OK**.

### Viewing an interface hierarchy

You can view an interface hierarchy using the Tree View dialog.

**Procedure**

1. On the Interfaces tab, select **Tree View**.
2. In the Tree View dialog, select the plus or minus boxes to expand or contract the tree view, which shows the hierarchy.
3. Select **Close** to exit the Tree View.

### Configuring network settings

You can use the Settings tab on the Network page to view and configure network settings.

#### Viewing network settings

You can view network settings for DD Management Center, while also adding or removing settings.

**Procedure**

1. Select **Administration > Settings > Network tab > Settings tab**.
2. View the network settings (described in the following table), and add or remove settings using the **Edit** button.

<table>
<thead>
<tr>
<th>Table 16 Network settings</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>item</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Host Name</td>
<td>Host name of selected DD system</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Fully qualified domain name associated with selected DD system</td>
</tr>
<tr>
<td><strong>Search Domain List</strong></td>
<td></td>
</tr>
<tr>
<td>Search Domain</td>
<td>List of search domains used by DD system. The DD system applies the search domain as a suffix to the host name.</td>
</tr>
<tr>
<td><strong>Hosts Mapping</strong></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of host to resolve</td>
</tr>
<tr>
<td>Host Name</td>
<td>Host names associated with IP address</td>
</tr>
<tr>
<td><strong>DNS List</strong></td>
<td></td>
</tr>
<tr>
<td>DNS IP Address</td>
<td>Current DNS IP addresses associated with selected DD system. An asterisk (*) means the IP addresses were assigned through DHCP.</td>
</tr>
</tbody>
</table>

### Setting host names

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

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 DD systems.

**Procedure**
1. Select *Administration > Settings > Network tab > Settings tab.*
2. In the Host Settings area, select *Edit.*
3. In the Configure Host dialog, select how you want to set the host and domain names:
   - Obtain Settings using DHCP.
   - Manually configure host.
     - Enter a host name.
     - Enter a domain name, which is the domain name associated with DD Management Center. Typically, this is your company domain name. For example, `yourcompany.com`
4. Select *OK.*

**Managing a domain search list**
You can add or remove a domain from a domain search list.

**Adding a search domain**
You can add a search domain using the Configure Search Domains dialog.

**Procedure**
1. Select *Edit* in the Search Domain List area.
2. In the Configure Search Domains dialog, select the add (+) button.
   a. In the Add Search Domain dialog, enter a name in the Search Domain text box.
   b. Select *OK.*
3. Select *OK.*

**Results**
Changes are applied to the system. The system returns you to the Settings view.

**Removing a search domain**
You can remove a search domain using the Configure Search Domains dialog.

**Procedure**
1. Select *Edit* in the Search Domain List area.
   a. In the Configure Search Domains dialog, select the search domain to remove.
   b. Select the remove (X) button.
2. Select *OK.*

**Results**
Changes are applied to the system. The system returns you to the Settings tab.
Mapping hosts

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

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

Procedure
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 a host name that will be used for the mapping in the Host Name box.
4. Select OK.
   The new host name is added to the list of Host Names. Continue to add host names as necessary.
5. In the Add Hosts dialog, enter the IP address that will be mapped to a host, then select the checkboxes of one or more host names from the list of hosts.
6. Select OK.
   The mapping is created, and you are returned to the Settings tab.

Deleting a host name mapping
You can delete a host name mapping using the Delete Host dialog.

Procedure
1. In the Settings view, select the checkbox of the host mapping to delete in the Hosts Mapping area.
2. Select Delete in the Hosts Mapping area.
   The Delete Host dialog appears.
3. Select Delete.
   Confirmation messages are displayed.
4. Select Close when the Completed message appears.
   You are returned to the Settings tab.

Managing DNS IP addresses
You can add or remove a DNS IP address.

Adding a DNS IP address
You can add a DNS IP address.

Procedure
1. Select Edit in the DNS List area.
2. In the Configure DNS dialog, 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:
  ▪ Select the plus (+) button.
  ▪ Enter the DNS IP address.
  ▪ Select OK.

Deleting a DNS IP address
You can delete a DNS IP address.

Procedure
1. Select the Manually configure DNS radio button.
2. Select the checkbox of the DNS IP address to delete.
3. Select the delete (X) button.
4. Select OK.

Configuring routes

Routes determine the path taken to transfer data to and from the local host (DD Management Center) to another network or host.

DD Management Center does not generate or respond to any of the network routing management protocols (RIP, EGRP/EIGRP, and BGP). The only routing implemented on DD Management Center 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).

DD Management Center 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 DD Management Center (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.

Viewing route information

The Routes pages provides details about all of the routing information for your DD Management Center setup, including the default gateway values, and static and dynamic routes.

Procedure
1. Select Administration > Settings > Network tab > Routes tab.
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

<table>
<thead>
<tr>
<th>Item</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default IPv4 Gateway</td>
<td>Address of the default IPv4 gateway.</td>
</tr>
</tbody>
</table>
Table 17 Route information (continued)

<table>
<thead>
<tr>
<th>item</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default IPv6</td>
<td>Address of the default IPv6 gateway.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Address of the default IPv6 gateway.</td>
</tr>
<tr>
<td>Static Routes</td>
<td>Static routes that are either network or host-based routes.</td>
</tr>
<tr>
<td>Route Spec</td>
<td>Route specification being used to configure routes.</td>
</tr>
<tr>
<td>Dynamic Routes</td>
<td>Dynamically assigned routes that use network or host paths for data</td>
</tr>
<tr>
<td></td>
<td>transmission.</td>
</tr>
<tr>
<td>Destination</td>
<td>Destination host/network where the network traffic (data) is sent.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Address of the router in the DD Management Center network or 0.0.0.0 if no</td>
</tr>
<tr>
<td></td>
<td>gateway is set.</td>
</tr>
<tr>
<td>Genmask</td>
<td>Netmask for the destination net. Initially set to 255.255.255.255 for a</td>
</tr>
<tr>
<td></td>
<td>host destination and 0.0.0.0 for the default route.</td>
</tr>
<tr>
<td>Flags</td>
<td>Possible values include:</td>
</tr>
<tr>
<td></td>
<td>U – Route is up.</td>
</tr>
<tr>
<td></td>
<td>H – Target is a host.</td>
</tr>
<tr>
<td></td>
<td>G – Use gateway.</td>
</tr>
<tr>
<td></td>
<td>R – Reinstate route for dynamic routing.</td>
</tr>
<tr>
<td></td>
<td>D – Dynamically installed by daemon or redirect.</td>
</tr>
<tr>
<td></td>
<td>M – Modified from routing daemon or redirect.</td>
</tr>
<tr>
<td></td>
<td>A – Installed by addrconf.</td>
</tr>
<tr>
<td></td>
<td>C – Cache entry.</td>
</tr>
<tr>
<td></td>
<td>! – Reject route.</td>
</tr>
<tr>
<td>Metric</td>
<td>Distance to target (usually counted in hops). (It is not used by the DD OS,</td>
</tr>
<tr>
<td></td>
<td>but might be needed by routing daemons.)</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transfer Unit (MTU) size for physical (Ethernet) interface.</td>
</tr>
<tr>
<td>Window</td>
<td>Default window size for TCP connections over this route.</td>
</tr>
<tr>
<td>IRTT</td>
<td>Initial RTT (Round Trip Time). The kernel uses this to estimate the best TCP</td>
</tr>
<tr>
<td></td>
<td>protocol parameters without waiting on (possibly slow) answers.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface name associated with routing interface.</td>
</tr>
</tbody>
</table>

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.

Procedure

1. Select Edit next to either the Default IPv4 Gateway or the Default IPv6 Gateway.
2. In the Configure Default IPv4/IPv6 Gateway dialog, choose how the gateway address is to be set:
   - Use DHCP value
     Indicates that you want to use the DHCP (Dynamic Host Configuration Protocol) server value.
• **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.

3. Select **OK**.
   The system processes the information and returns you to the Routes tab.

### 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 will override source routing.

**Procedure**

1. Select **Create** in the Static Routes area.
2. In the Create Routes dialog, select an interface, and select **Next**.
3. Specify the **Destination** by selecting one of the following:
   - **Network** – Enter the network IP address and netmask.

   **Note**
   This is not the IP address of the interface. The interface was selected in the initial dialog, and it is used for routing traffic.

   - **Host** – Enter the host name or IP address of the destination host of the route.

4. Optionally, enter a new gateway address in the **Gateway** box.
5. Select **Next**.
6. Review your changes on the Summary page, and select **Finish**.
   Progress messages are displayed. When the changes are applied, the message indicates Completed.
7. Select **OK** to close the dialog.
   The new route specification is listed in the Route Spec list under Static Routes.

### Deleting static routes

You can delete static routes when you no longer need them.

**Procedure**

1. In the **Route Spec** area, select the checkbox of the route specification to delete.
2. Select **Delete**.
   The Delete Route dialog appears.
3. Select **Delete** and **Close**.
   The selected route specification is removed from the Route Spec list.
Upgrading DD Management Center software

Only DD Management Center admins have permission to manage software upgrade packages and perform upgrades for DD Management Center.

Upgrading DD Management Center software is done in two stages:

- Obtaining an image from EMC Online Support, or selecting a previously obtained upgrade image that has been saved.
- Performing the upgrade on the DD Management Center.

Managing DD Management Center upgrade packages

You can download an upgrade image from EMC Online Support to a locally accessible drive and then add it to the upgrade package collection managed by DD Management Center.

Procedure

1. Select Administration > Settings > Upgrade tab.
2. In the Upgrade Packages Available on Data Domain System 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, select the EMC Online Support link.
   - To upload a package that has been stored locally to the inventory, select Upload Upgrade Package, and browse to the local drive to select the package.
   - To delete a package, select the package from the inventory list, and select Remove Upgrade Package.
3. To perform the upgrade, see the procedure in the following section.

Performing a DD Management Center software upgrade

After you have uploaded an upgrade package, you can use it to upgrade your DD Management Center software.

**Note**

Software upgrade files use the .rpm file extension. This topic assumes that you are updating only DD Management Center. 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.

Procedure

1. Review the appropriate DD Management Center 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. Select Administration > Settings > Upgrade tab.
3. In the Upgrade Packages Available on Data Domain System area, select the upgrade package from the list, and select Perform System Upgrade.
4. Monitor the upgrade progress from the DD Management Center console page.
5. Be aware that the upgrade process automatically reboots DD Management Center.
6. It is recommended that you keep the System Upgrade progress dialog open until the upgrade completes, or until the system powers off.

Checking a DD Management Center serial number

Each DD Management Center virtual machine has a unique serial number, which is used to identify the system in autosupport messages.

1. Select Administration > Settings > Serial Number tab.
2. View the serial number listed.
3. To change the serial number, select Edit.
4. In the Edit dialog, enter the new serial number, and select Submit.

Note

DD Management Center does not require a license, but the managed DD systems must have licenses for their core and optional features.

Managing alerts

You can configure settings to determine who will receive DD Management Center alert notifications and daily alert summaries.

DD Management Center and DD systems (DD OS) use the same alert system. Detailed information about the alert system is described in the EMC Data Domain Operating System Administration Guide.

Managing alert notifications

The groups that are configured to receive DD Management Center alert notifications are listed in the Administration > Settings > Alerts page with the Notification 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.

Procedure

1. Select Administration > Settings > Alerts tab > Notifications tab > Add.
2. In the Add Group dialog, type a name for the group in the Group Name text box.

3. Select the alert class attributes, set the severity level at which notifications are to be sent, and select **OK**.

   For example, you could create a CriticalWarnings group, select all classes, and set the severity level to Critical.

4. Select the checkbox of the group, now in the Notifications group list, and select **Modify**.

5. In the Modify Group dialog, select **Subscribers**, and in the Subscribers panel, select **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 select **Finish**.

**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.

**Procedure**

1. In the **More Tasks** menu, select **Send Test Alert**.

2. In the Notification Groups panel, select the checkboxes 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.

**Procedure**

1. Select the checkbox 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.

**Procedure**

1. Select one or more checkboxes 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.

**Procedure**

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.

Procedure
1. Select Administration > Settings > Alerts tab > Notification tab.
2. Select the checkbox of the desired group, and select Configure in the Subscribers area.
3. In the Edit Subscribers dialog, select one of the following options:
   - To add a subscriber, select Add (green plus sign). Enter the email address in the Email Address dialog, and select OK.
   - To modify an email address, select the checkbox of the email address in the Subscriber Email list, and select Modify (pencil). Edit the email address in the Email Address dialog, and select OK.
   - To delete an email address, select the checkbox of the email address in the Subscriber Email list, and select Delete (X).
4. Select OK.

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.

Procedure
1. Select Administration > Settings > Alerts tab > Daily Alert Summary tab.
2. If the default “8:00 AM Daily” delivery time is not acceptable, select Schedule.
3. In the Schedule Alert Summary dialog, select the hour, minute, and AM/PM, and select OK.
4. Select Configure/Edit in the Subscribers area to display the Daily Alert Summary Mailing List dialog.
5. Manage the subscriber email:
   - To add a subscriber, select Add (green plus sign), enter the email address in the Email Address dialog, and select OK.
   - To modify an email address, select the checkbox of the email address in the Subscriber Email list, and select Modify (pencil). Edit the email address in the Email Address dialog, and select OK.
   - To delete an email address, select the checkbox of the email address in the Subscriber Email list, and select Delete (X).
Managing general configuration settings

Under the Administration > Settings > General tab, you can manage settings for your mail server, how time and date are obtained, some system properties (location and default administrator's email and host name), and SNMP properties.

Configuring mail server settings

You can set or change the name of your mail server using the Set Mail Server dialog.

Procedure

1. Select Administration > Settings > General tab > Mail Server tab > More Tasks > Set Mail Server.
2. In the Set Mail Server dialog, enter the name of the mail server, and select OK.

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)], using the Configure Time Settings dialog.

Procedure

1. Select Administration > Settings > General tab > Time and Date Settings tab > More Tasks > Configure Time Settings.
2. In the Configure Time Settings dialog, select the Time Zone drop-down list, and select the time zone where DD Management Center resides.
3. Set how time is synchronized:
   - To manually set the time and date, select None, enter 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.
4. Select OK.

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 Set System Properties dialog.

Procedure

2. In the Set System Properties dialog, the Location text field shows where the system is located. [This text field is not used by DD Management Center (or DD OS); it is here simply for your information.]
3. In the Admin Email text box, enter an email address to be automatically added to the alert and autosupport notification lists.
4. In the Admin Host text box, enter 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.

5. Select OK.

Working with SNMP

To monitor DD Management Center using SNMP, you will need to install the Data Domain MIB in your SNMP Management system. The Data Domain MIB will allow SNMP queries for Data Domain-specific information.

DD Management Center 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.

DD Management Center 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.

Checking SNMP status and configuration

The SNMP page shows SNMP status and properties, and the SNMP V3 and SNMP V2C configuration.

1. Select Administration > Settings > General tab > SNMP tab.

2. View information about SNMP, as described in the following tables.

<table>
<thead>
<tr>
<th>Table 18 SNMP status</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>item</strong></td>
</tr>
<tr>
<td>Status</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 19 SNMP properties</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>item</strong></td>
</tr>
<tr>
<td>SNMP System Location</td>
</tr>
<tr>
<td>SNMP System Contact</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 20 SNMP V3 configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>item</strong></td>
</tr>
<tr>
<td>SNMP Users</td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Access</td>
</tr>
</tbody>
</table>
### Table 20 SNMP V3 configuration (continued)

<table>
<thead>
<tr>
<th>item</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Authentication protocol for validating SNMP user:</td>
</tr>
<tr>
<td>Protocols</td>
<td>- MD5</td>
</tr>
<tr>
<td></td>
<td>- SHA1</td>
</tr>
<tr>
<td>Privacy Protocol</td>
<td>Encryption protocol for validating SNMP user:</td>
</tr>
<tr>
<td></td>
<td>- AES</td>
</tr>
<tr>
<td></td>
<td>- DES</td>
</tr>
<tr>
<td></td>
<td>- None</td>
</tr>
<tr>
<td>Trap Hosts</td>
<td>Host IP address or domain name of the SNMP management host.</td>
</tr>
<tr>
<td></td>
<td>Port Port used for SNMP trap communication with the host. Port 162 is the</td>
</tr>
<tr>
<td></td>
<td>default.</td>
</tr>
<tr>
<td></td>
<td>User User on trap host authenticated to access Data Domain SNMP information.</td>
</tr>
</tbody>
</table>

### Table 21 SNMP V2C configuration

<table>
<thead>
<tr>
<th>item</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communities</td>
<td>Name of the community, for example, public, private, or localCommunity.</td>
</tr>
<tr>
<td>Community</td>
<td>Access permission assigned. This can be:</td>
</tr>
<tr>
<td>Access</td>
<td>- Read-only</td>
</tr>
<tr>
<td>Hosts</td>
<td>The hosts in this community.</td>
</tr>
<tr>
<td>Trap Hosts</td>
<td>Systems designated to receive SNMP traps generated by DD Management Center.</td>
</tr>
<tr>
<td>Host</td>
<td>If this parameter is set, systems receive alert messages, even if the</td>
</tr>
<tr>
<td></td>
<td>SNMP agent is disabled.</td>
</tr>
<tr>
<td>Port</td>
<td>Port used for SNMP trap communication with the host. Port 162 is the</td>
</tr>
<tr>
<td>Community</td>
<td>default.</td>
</tr>
<tr>
<td></td>
<td>Name of the community, for example, public, private, or localCommunity.</td>
</tr>
</tbody>
</table>
Enabling or disabling SNMP

You can enable or disable SNMP through DD Management Center.

Procedure
1. In the Status area, select Enable to use SNMP.
2. In the Status area, select Disable to stop using SNMP.

Downloading the SNMP MIB

You can download the SNMP MIB through DD Management Center.

Procedure
1. In the Status area, select Download MIB file.
2. In the Opening DATA_DOMAIN.mib dialog, select Save.

Configuring SNMP properties

You can configure SNMP system location and system contacts.

Procedure
1. In the SNMP Properties area, select Configure.
2. In the SNMP Configuration dialog, in the text fields, add an SNMP system location (a description of where DD Management Center is located) and/or an SNMP system contact (for example, the email address of the system administrator for DD Management Center).
3. Select OK.

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 DD Management Center.

Creating SNMP V3 users

You can set up SNMP V3 users using the Create SNMP User dialog.

Procedure
1. In the SNMP Users area, select Create.
   The Create SNMP 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 DD Management Center. 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 OK.
   The newly added user account appears in the SNMP Users table.

Modifying SNMP V3 users
You can modify a variety of information about SNMP V3 users.
Procedure
1. In the SNMP Users area, select a checkbox for the user, and select Modify. 
   In the Modify SNMP User dialog, add or change any of the settings.
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 OK.
   The new settings for this user account are displayed in the SNMP Users table.

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.
Procedure
1. In the SNMP Users area, select a checkbox for the user, and select Delete.
   The Delete SNMP Users dialog box appears.
2. Verify the user name to be deleted, and select OK.
   
   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.
3. In the Delete SNMP User Status dialog box, select Close.
   The user account is removed from the SNMP Users table.
Managing SNMP V3 and V2C trap hosts

Managing SNMP V3 and V2C trap hosts includes creating, modifying, and removing hosts that received SNMP traps.

Creating SNMP V3 and V2C trap hosts

You can create SNMP V3 and V2C trap hosts.

Procedure

1. In the SNMP V3 Trap Hosts or SNMP V2C Trap Hosts area, select Create.
   The Create 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 OK.

Modifying SNMP V3 and V2C trap hosts

You can modify the port, user, and/or community for an SNMP V3 or V2C trap host.

Procedure

1. In the Trap Hosts area (either for V3 or V2C), select a Trap Host entry and select Modify.
   The Modify 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 OK.

Removing SNMP V3 and V2C trap hosts

You can remove SNMP V3 and V2C trap hosts.

Procedure

1. In the Trap Hosts area (either for V3 or V2C), select a trap host entry, and select Delete.
   The Delete SNMP [V3 or V2C] Trap Hosts dialog appears.

2. Verify the host name to be deleted, and select OK.

3. In the Delete SNMP [V3 or V2C] Trap Hosts Status dialog, select Close.
   The trap host entry is removed from the Trap Hosts table.
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.

Creating SNMP V2C communities
You can create SNMP V2C communities.

Procedure
1. In the Communities area, select Create.
   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 DD Management Center. 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 OK.
   The new community entry appears in the Communities table.

Modifying SNMP V2C communities
You can modify SNMP V2C communities.

Procedure
1. In the Communities area, select a checkbox for the community, and select Modify.
   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 OK.
   The modified community entry appears in the Communities table.
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.

Procedure

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. In the Delete SNMP V2C Communities dialog, verify the community name to be deleted, and select **OK**.

3. In the Delete SNMP V2C Communities Status dialog, select **Close**. The community entry is removed from the Communities table.

Managing autosupport reporting

The autosupport reporting feature emails an automatically generated daily report, called an ASUP, to EMC Data Domain Support.

This report shows DD Management Center 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 DD systems in this report.

Autosupport reporting is enabled by default. To disable it:

1. Select **Administration** > **Settings** > **Support tab** > **Autosupport tab**.
2. In the Vendor Support area, select **Disable**.

   **Note**
   
   For more information about autosupport reporting, see the *EMC Data Domain Operating System Administration Guide*.

Using ConnectEMC or legacy email for autosupport

By default, autosupport reports are enabled and sent daily to EMC Data Domain Customer Support using the *legacy email method*. The *ConnectEMC method* sends messages in a secure format using email, FTP, or HTTPS.

To determine if autosupport reporting is currently enabled, and if so, the method in use:

Procedure

1. Select **Administration** > **Settings** > **Support tab** > **Autosupport tab**.
2. In the Vendor Support area, is Notification Status is Enabled, you will see either **ConnectEMC** (with email, FTP, or HTTPS) or simply an email address, which means the current method is the legacy email method.
3. To change the method, see the *EMC Data Domain Operating System Administration Guide*.
Adding to the autosupport report email list

By default, autosupport reports are enabled and sent daily to EMC Data Domain Customer Support. You may want to add additional email addresses as recipients of autosupport reports.

Procedure

1. Select Administration > Settings > Support tab > Autosupport tab.
2. In the Autosupport Mailing List area, select Configure.
3. In the Configure Autosupport Subscribers dialog, select Add (green + sign) to open the Email dialog.
4. Enter a recipient's email address in the text box, and select OK.
5. Select OK to exit the Configure Autosupport Subscribers dialog.

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, EMC Data Domain 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. Select Administration > Settings > Support tab > Support Bundles tab.
2. Select Generate Support Bundle.
3. When you see the new .tar.gz file, email it to EMC Data Domain Support. If it is too large to be emailed, go to the EMC Data Domain Support site, and upload it.

Managing system logs

A messages file and audit log file are saved on DD Management Center and listed in the Logs area. Files can be opened and saved to a local location and then forwarded to support, if required.

Procedure

1. Select Administration > Settings > Logs.

2. 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.
3. Save the log file locally, if needed.
APPENDIX A

Graphics Reference for DD Management Center

- Global controls and icons........................................................................................................118
- Dashboard controls..................................................................................................................120
- Widget controls......................................................................................................................120
- Group icons..........................................................................................................................121
- Property controls..................................................................................................................122
Global controls and icons

The controls and icons that are used throughout the DD Management Center interface are described in detail.

Table 22 Controls that perform a function

<table>
<thead>
<tr>
<th>control</th>
<th>name</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help</td>
<td>Located in the DD Management Center banner, opens the top-level help page. The help is derived from the <em>EMC Data Domain Management Center User Guide</em>.</td>
<td></td>
</tr>
<tr>
<td>About DD</td>
<td>Displays an information page, showing the details of this version of DD Management Center.</td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>Center</td>
<td></td>
</tr>
<tr>
<td>Log Out</td>
<td>Located in the DD Management Center banner, logs you out of DD Management Center.</td>
<td></td>
</tr>
<tr>
<td>Filter controls</td>
<td>The filter control is comprised of two parts: the funnel icon and a drop-down menu. When the funnel icon is selected, it toggles filtering on or off.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If filtering is being performed, selecting the funnel turns all filtering off, causing all systems to be visible.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If filtering is off, selecting the funnel turns filtering on, using the previously set filter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When a filter is active, the funnel display is yellow. Select Show Filter or the Filtered by link to see details about what is filtered.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Filter selection is performed with the small down arrow, which opens a drop-down list of the types of filtering that can be employed:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Filter by group – Enables the selection of one or more groups. Systems belonging to the selected groups display in the work area panel.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Filter by property – Enables the selection of one or more property values. Systems having those property values display in the work area panel.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Filter by system – Enables the selection of one or more systems to be displayed in the work area panel.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Filtering is used in the work area panel for monitoring views, and for Reports and Dashboard widgets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View by System (default) – Displays systems as a flat list, whose entries are sortable using the table column sorting controls.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>
### Table 22 Controls that perform a function (continued)

<table>
<thead>
<tr>
<th>control</th>
<th>name</th>
<th>description</th>
</tr>
</thead>
</table>
| ⚙️ ⚙️ ⚙️ | System, Group, Tenant view toggle | Same as the previous icon, but you can also select:  
- **View by Tenant** (default) – Displays tenants as a flat list, whose entries are sortable using the table column sorting controls. |
| 🔗 | Launch DD System Manager | Starts DD System Manager in a new browser window for the selected system, where you can directly manage or investigate the corresponding area from where it was launched. |
| ♂️ | 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, etc), based on the column data type. |
| + | Add | Opens a dialog 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 DD Management Center. On the Administration > Properties page, this lets you to create custom properties for managed objects. |
| ✎ | Edit | For a selected table element, opens a dialog 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. |

You can select the icon to display a status banner with more information about the connection problem.

### Table 23 Icons showing system and/or connection status

<table>
<thead>
<tr>
<th>icon</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="icon" /></td>
<td>Normal – Communication between DD Management Center and the DD system is operating normally.</td>
</tr>
<tr>
<td><img src="image2.png" alt="icon" /></td>
<td>Unreachable – The DD system is not responding or is not transmitting. Data was last retrieved as of the date shown in the status banner.</td>
</tr>
<tr>
<td><img src="image3.png" alt="icon" /></td>
<td>Unmanaged – The DD system is suspended or unmanaged. When suspended, all data collection ceases. A system is suspended when management has been taken over by another DD Management Center or when the system is suspended using the CLI.</td>
</tr>
<tr>
<td><img src="image4.png" alt="icon" /></td>
<td>Adding – The DD system is being added into the inventory.</td>
</tr>
<tr>
<td><img src="image5.png" alt="icon" /></td>
<td>Upgrading – The DD system is being upgraded and is unavailable during this state.</td>
</tr>
</tbody>
</table>
Table 23 Icons showing system and/or connection status (continued)

<table>
<thead>
<tr>
<th>icon</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄</td>
<td>Synchronizing – Data for the DD system is being synchronized. The system is unavailable during this state.</td>
</tr>
<tr>
<td>📑</td>
<td>Unsupported system – This system is unsupported because it is running an operating system that is not supported by this version of DD Management Center. 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.</td>
</tr>
</tbody>
</table>

Table 24 Icons for Tenants and Tenant Units

<table>
<thead>
<tr>
<th>icon</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td>🏠</td>
<td>Tenant Unit Configuration Issues – Reported in all multitenancy 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.</td>
</tr>
</tbody>
</table>

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 your Data Domain environment.

Table 25 Dashboard controls

<table>
<thead>
<tr>
<th>controls</th>
<th>name</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📕</td>
<td>Add Widget</td>
<td>Opens the Add Dashboard Widget dialog where you can select a widget template and optional filters to create a widget.</td>
</tr>
<tr>
<td>📕</td>
<td>Add/Configure Tabs</td>
<td>Opens the Add and Configure Dashboard Tabs dialog 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.</td>
</tr>
<tr>
<td>📕</td>
<td>Maximize/Restore dashboard</td>
<td>Toggles the size of the dashboard. Maximize hides the navigation panel and Restore returns to default view, exposing the navigation panel.</td>
</tr>
</tbody>
</table>

Widget controls

Each widget includes the following standard controls.

<table>
<thead>
<tr>
<th>controls</th>
<th>name</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📕</td>
<td>Edit Widget</td>
<td>Opens the Edit Dashboard Widget where you can change the widget name and filter criteria, and in some cases, widget details.</td>
</tr>
</tbody>
</table>
### Group icons

On the Administration > Groups page, the DD Management Center system administrator creates groups in a tree-like hierarchy for logically organizing DD systems.

**Table 26 Group icons**

<table>
<thead>
<tr>
<th>controls</th>
<th>name</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Group</strong></td>
<td>Symbolizes a group containing DD 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Group with permissions applied</strong></td>
<td>Indicates that this group is controlled by access permissions.</td>
</tr>
<tr>
<td></td>
<td><strong>Membership details</strong></td>
<td>Appears when a DD system belongs to more than one group. Hover to view the names of groups of which this DD system is a member.</td>
</tr>
</tbody>
</table>
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 27 Property controls

<table>
<thead>
<tr>
<th>controls</th>
<th>name</th>
<th>description</th>
</tr>
</thead>
</table>
|            | 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:  
  - 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.            |
|            | Property 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. |
|            | Info          | Opens the Property Assignment dialog, from the Edit Property dialog, and lists the type of property, the name of the element (for example, system name), and assigned value. |
APPENDIX B

Command Line Interface for DD Management Center

- Differences between DDMC CLI and DD OS CLI .......................................................... 124
- Tasks available only in DDMC CLI ........................................................................ 124
- managed-system commands ................................................................................. 124
- task commands ..................................................................................................... 129
Differences between DDMC CLI and DD OS CLI

The DD Management Center CLI (command line interface) was derived from the DD OS (Data Domain Operating System) CLI, but has been modified to fit the needs and tasks of DD Management Center.

- There are two unique DD Management Center 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 DD Management Center; however, some arguments and output are not included because DD Management Center 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 DD Management Center, 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 DD Management Center GUI for all system management tasks. However, you must use the DD Management Center 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 DD Management Center, 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]`

managed-system commands

The DD Management Center 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 DD system to the set of managed DD 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 DD system from the other DD Management Center, and the DD 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 DD system is through a proxy.

**inbound-proxy-port proxy-port**
Inbound proxy port number if the incoming connection from the DD system is through a proxy.

**outbound-proxy proxy-host**
Outbound proxy host name if the connection from the DD Management Center to the DD system is through a proxy.

**outbound-proxy-port proxy-port**
Outbound proxy port number if the connection from the DD Management Center to the DD system is through a proxy.

---

**Note**
The proxy options are equivalent to the firewall options in the graphical user interface.

---

**Example**

```
# managed-system add host1234.mycompany.com
The SHA1 fingerprint for the remote host's CA certificate is
Do you want to trust this certificate? Are you sure? (yes|no) [no]: yes
** Once added, all "admin" role users on this management center will
operate on "host1234.mycompany.com" system with "admin" role. To allow
"host1234.mycompany.com" to be managed by this management center, Enter sysadmin password:
ok, proceeding.
```
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 DD Management Center. Use managed-system add to add the system to the set of systems that this DD Management Center 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 DD system is through a proxy.

inbound-proxy-port proxy-port
   Inbound proxy port number if the incoming connection from the DD system is through a proxy.

outbound-proxy proxy-host
   Outbound proxy host name if the connection from the DD Management Center to the DD system is through a proxy.

outbound-proxy-port proxy-port
   Outbound proxy port number if the connection from the DD Management Center to the DD system is through a proxy.

managed-system delete

managed-system delete hostname

This command removes the specified DD system from DD Management Center 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 DD 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 DD 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 DD system is through a proxy.

**outbound-proxy {proxy-host|none}**
Outbound proxy host name if the connection from the DD Management Center to the DD 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 DD 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 DD Management Center is in the process of assuming management of the system.

**deleting**
The DD Management Center is in the process of ending management of the system.

**managed**
The DD Management Center is managing the system.
suspended
The DD Management Center 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 DD Management Center previously managed the system, but another DD Management Center has assumed management.

unsupported
This system is unsupported, because its DD OS version is not supported by this version of DD Management Center.

Management Status Values of “Managed” Systems
This list describes the possible management Status values when a system is in the managed state.

not-responding
DD Management Center 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 DD Management Center 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 DD Management Center.

managed-system suspend
managed-system suspend hostname

This command suspends data collection from the specified host. If you do not want DD Management Center 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 DD Management Center 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 DD Management Center, 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}

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.

**task show detailed**

`task show detailed task-id`

This command prints a detailed report about a single task and its subtasks.

**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}**  
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.

**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}**  
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.
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.