## Appendix A  Time Zones

<table>
<thead>
<tr>
<th>Region</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Zones Overview</td>
<td>46</td>
</tr>
<tr>
<td>Africa</td>
<td>46</td>
</tr>
<tr>
<td>America</td>
<td>46</td>
</tr>
<tr>
<td>Antarctica</td>
<td>47</td>
</tr>
<tr>
<td>Asia</td>
<td>47</td>
</tr>
<tr>
<td>Atlantic</td>
<td>48</td>
</tr>
<tr>
<td>Australia</td>
<td>48</td>
</tr>
<tr>
<td>Brazil</td>
<td>48</td>
</tr>
<tr>
<td>Canada</td>
<td>48</td>
</tr>
<tr>
<td>Chile</td>
<td>48</td>
</tr>
<tr>
<td>Etc</td>
<td>48</td>
</tr>
<tr>
<td>Europe</td>
<td>49</td>
</tr>
<tr>
<td>GMT</td>
<td>49</td>
</tr>
<tr>
<td>Indian (Indian Ocean)</td>
<td>49</td>
</tr>
<tr>
<td>Mexico</td>
<td>49</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>50</td>
</tr>
<tr>
<td>Pacific</td>
<td>50</td>
</tr>
<tr>
<td>System V</td>
<td>50</td>
</tr>
<tr>
<td>US (United States)</td>
<td>50</td>
</tr>
<tr>
<td>Aliases</td>
<td>50</td>
</tr>
</tbody>
</table>

## Appendix B  EMC Data Domain System Security Configuration

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Domain System Security Overview</td>
<td>52</td>
</tr>
<tr>
<td>Security Configuration Settings</td>
<td>52</td>
</tr>
<tr>
<td>Access Control Settings</td>
<td>53</td>
</tr>
<tr>
<td>Log Settings</td>
<td>58</td>
</tr>
<tr>
<td>Communication Security Settings</td>
<td>59</td>
</tr>
<tr>
<td>Data Security Settings</td>
<td>64</td>
</tr>
<tr>
<td>Secure Serviceability Settings</td>
<td>65</td>
</tr>
<tr>
<td>Security Alert System Settings</td>
<td>66</td>
</tr>
<tr>
<td>EMC Data Domain Retention Lock Software</td>
<td>66</td>
</tr>
<tr>
<td>Dual Sign-On Requirements</td>
<td>66</td>
</tr>
<tr>
<td>Secure System Clock</td>
<td>66</td>
</tr>
<tr>
<td>Secure Maintenance: Data Migration</td>
<td>66</td>
</tr>
<tr>
<td>Physical Security Controls</td>
<td>67</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 product 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 Data Domain Support Portal (https://my.datadomain.com/) to ensure that you are using the latest version of this document.

Purpose
This guide explains how to perform the initial configuration of an EMC Data Domain system.

This preface includes descriptions of related documentation, conventions, audience, and contact information.

Audience
This guide is for system administrators who are responsible for performing the initial configuration of an EMC Data Domain system.

Related Documents
The EMC Data Domain Installation and Setup Guide, which is shipped with your Data Domain system, provides instructions for installing your Data Domain system, connecting it to an administrative console, and powering it on. After you have completed installing and powering on your system, refer to this guide for additional information.

The following Data Domain system documentation provides additional information about the use of the system:

- EMC Data Domain Operating System Release Notes for your DD OS version
- EMC Data Domain Operating System Administration Guide
- EMC Data Domain Operating System Command Quick Reference
- EMC Data Domain Operating System Command Reference Guide
- EMC Data Domain Hardware Guide
- EMC Data Domain Expansion Shelf Hardware Guide
  (There is a guide for each of the shelf models: the ES20 and ES30.)
- EMC Data Domain Boost for OpenStorage Administration Guide
- EMC Data Domain Extended Retention Administration Guide
- The EMC Data Domain system installation and setup guides for each of the supported platforms.

Access Integration-Related Documents
The Documentation page at https://my.datadomain.com/documentation provides access to three categories of documents that are related to the use of Data Domain products:

- User guides, under Product Documentation.
- Guides for how to integrate Data Domain systems with backup applications, under Integration Documentation.
- Matrices that show which components are compatible with each other, under Compatibility Matrices:
  - Data Domain hardware product numbers
  - Data Domain operating system (DD OS) versions
  - Backup software versions
  - Backup software server and client operating system versions
  - Hardware driver versions

Access Data Domain Documents
1. Log into the support portal at: https://my.datadomain.com/documentation.
2. To view user documents, click Product Documentation and then perform the following steps:
   a. Select the Data Domain model from the Platform list and click View.
   b. On the row for the correct Data Domain operating system (DD OS) version, Click View under Documentation.
   c. Click the desired title.
3. To view integration-related documents, perform the following steps:
   a. Click Integration Documentation.
   b. Select a vendor from the Vendor menu.
   c. Select the desired title from the list and click View.
4. To view compatibility matrices, perform the following steps:
   a. Click Compatibility Matrices.
   b. Select the desired title from the product menu and click View.

Special Notice Conventions Used in This Document
EMC uses the following conventions for special notices:

⚠️ **DANGER**
Indicates a hazardous situation which, if not avoided, will result in death or serious injury.

⚠️ **WARNING**
Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

⚠️ **CAUTION**
Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

💡 **NOTICE**
Addresses practices not related to personal injury.

**Note**
Presents information that is important, but not hazard-related.
Typographical conventions
EMC uses the following type style conventions in this document:

**Bold**
Use for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)

*Italic*  Use for full titles of publications referenced in text

**Monospace**
Use for:
- System code
- System output, such as an error message or script
- Pathnames, filenames, prompts, and syntax
- Commands and options

*Monospace italic*  Use for variables

*Monospace bold*  Use for user input

[]  Square brackets enclose optional values

|  Vertical bar indicates alternate selections - the bar means “or”

{}  Braces enclose content that the user must specify, such as x or y or z

...  Ellipses indicate nonessential information omitted from the example

Contacting Data Domain
To resolve issues with Data Domain products, contact your contracted support provider or visit us online at https://my.datadomain.com/
The EMC Data Domain Operating System (DD OS) is pre-installed on the EMC Data Domain system. You need to configure the DD OS for your installation using one of two configuration wizards. One wizard is available through a Web-based browser (the Data Domain System Manager), and the other wizard uses the command-line interface (CLI).

Note

The Data Domain System Manager was formerly known as the Enterprise Manager.

When the configuration is complete, your system is ready to back up data.

This chapter covers the following topics:

- Prerequisites ........................................................................................................... 10
- Installation and Configuration Overview ................................................................. 12
**Prerequisites**

This guide assumes the following tasks have been completed:

**Procedure**

1. The Data Domain system has been completely installed and is ready to be powered on as described in your system's *EMC Data Domain Installation and Setup Guide*.

2. An administrative console has been set up to communicate with the system as described in the *EMC Data Domain Installation and Setup Guide*. You can use either a serial console or a monitor and keyboard, depending on your system model.

**Obtain this Information Before You Start**

**Procedure**

1. For NFS clients: Contact your Data Domain Systems Engineer about setting up the NFS server behind a firewall.

2. Have the information described in the next table available for you to enter during the configuration procedure.

<table>
<thead>
<tr>
<th>Required</th>
<th>Description</th>
<th>Your Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default user account</td>
<td>sysadmin. During the initial configuration the sysadmin is prompted to change the password. The sysadmin account cannot be deleted.</td>
<td><code>sysadmin</code></td>
</tr>
<tr>
<td>Login default password</td>
<td>This value is the Data Domain system's serial number or service tag number.</td>
<td></td>
</tr>
<tr>
<td>Licenses</td>
<td>A license consists of characters in this format:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ABCD-ABCD-ABCD-ABCD.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ABCD-ABCD-ABCD-ABCD-ABCD (for systems with EMC serial numbers)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ABCD-ABCD-ABCD-ABCD-ABCD-ABCD-AB (DD OS 5.1 and later for shelf capacity licenses)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For more information, see <a href="#">dd_c_about_licenses on page 11</a>.</td>
<td></td>
</tr>
<tr>
<td>If using the Dynamic Host Configuration Protocol (DHCP), obtain the MAC address of the network port.</td>
<td>The Media Access Control (MAC) address consists of 12 alphanumeric characters. This information is used to configure the DHCP server that assigns an IP address for the Data Domain system. The MAC address is printed on a label and should be visible. Its location varies according to system model.</td>
<td></td>
</tr>
</tbody>
</table>

3. If you are not using DHCP, determine the values listed in the next table, which you need to enter during the configuration procedure.
### Required

<table>
<thead>
<tr>
<th>Required</th>
<th>Notes</th>
<th>Your Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface IP addresses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface netmasks</td>
<td>You can configure different network interfaces on a Data Domain system to different subnets.</td>
<td></td>
</tr>
<tr>
<td>Routing gateway IP address</td>
<td>The IP address of the routing gateway.</td>
<td></td>
</tr>
<tr>
<td>If using DNS, the list of DNS servers</td>
<td>A comma-separated list of IP addresses of your DNS servers.</td>
<td></td>
</tr>
<tr>
<td>Site domain name</td>
<td>The domain name of the system, such as company.com.</td>
<td></td>
</tr>
<tr>
<td>A fully qualified hostname for the Data Domain system</td>
<td>The hostname of the system that includes the domain name, such as dd01.company.com.</td>
<td></td>
</tr>
</tbody>
</table>

4. If using a Fibre Channel transport, obtain the WWN numbers.

World-Wide Name (WWN) is a unique identifier in the Fibre Channel (FC) environment. It is used for zoning in SAN fabrics and LUN masking in storage arrays to manage storage access. A system has at least one World-Wide Node Name (WWNN), and each Fibre Channel port also has at least one World-Wide Port Name (WWPN). A WWN typically contains the Organization Unique Identifier (OUI), which is registered with and assigned by IEEE.

5. If you will be configuring your Data Domain system to interface with a VLAN, the VLAN IP addresses should be collected.

### About Licenses

Optional Data Domain software and hardware upgrades require a license.

**Table 1** Features Requiring Licenses

<table>
<thead>
<tr>
<th>Feature/License Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMC Data Domain ArchiveStore</td>
<td>Licenses Data Domain systems for archive use, such as file and email archiving, file tiering, and content and database archiving.</td>
</tr>
<tr>
<td>EMC Data Domain Boost</td>
<td>Enables the use of a Data Domain system with the following applications: EMC Avamar, EMC NetWorker, Oracle RMAN, Quest vRanger, Symantec Veritas NetBackup (NBU), and Backup Exec. The managed replication feature of DD Boost also requires the DD Replicator license.</td>
</tr>
<tr>
<td>EMC Data Domain Encryption</td>
<td>Allows data on system drives or external storage to be encrypted while being saved, and then locked before moving it to another location.</td>
</tr>
<tr>
<td>EMC Data Domain Expansion Storage</td>
<td>Allows external shelves to be added to the Data Domain system for additional capacity.</td>
</tr>
</tbody>
</table>
Table 1 Features Requiring Licenses (continued)

<table>
<thead>
<tr>
<th>Feature/License Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMC Data Domain Extended Retention (formerly DD Archiver)</td>
<td>Licenses the Extended Retention storage feature. See GUID-35AAB5AD-4619-42F9-B295-E3C634CB2ACD for additional information.</td>
</tr>
<tr>
<td>EMC Data Domain I/OS (for IBM i operating environments)</td>
<td>An I/OS license is required when VTL is used to backup systems in the IBM i operating environment. Apply this license before adding virtual tape drives to libraries.</td>
</tr>
<tr>
<td>EMC Data Domain NDMP Tape Server</td>
<td>Enables the use of a Data Domain system as a virtual tape library that supports backups of NAS devices over Ethernet/IP networks.</td>
</tr>
<tr>
<td>EMC Data Domain Replicator</td>
<td>Adds DD Replicator for replication of data from one Data Domain system to another. A license is required on each system.</td>
</tr>
<tr>
<td>EMC Data Domain Retention Lock Compliance Edition</td>
<td>Meets the strictest data retention requirements from regulatory standards such as SEC17a-4.</td>
</tr>
<tr>
<td>EMC Data Domain Retention Lock Governance Edition</td>
<td>Protects selected files from modification and deletion before a specified retention period has expired.</td>
</tr>
<tr>
<td>EMC Data Domain Shelf Capacity</td>
<td>Enables a Data Domain system to expand the active tier storage capacity beyond the entry capacity defined for that system.</td>
</tr>
<tr>
<td>EMC Data Domain Virtual Tape Library (VTL)</td>
<td>Enables the use of a Data Domain system as a virtual tape library over a Fibre Channel network.</td>
</tr>
<tr>
<td>Gateway Expanded Storage Level 2</td>
<td>Enables gateway systems to support additional usable capacity.</td>
</tr>
<tr>
<td>Gateway Expanded Storage Level 3</td>
<td>Enables gateway systems to support additional capacity greater than Expanded Storage Level 2 usable capacity.</td>
</tr>
</tbody>
</table>

Also see the Release Notes for information about new features that require a license.

Installation and Configuration Overview

The steps for the installation and initial configuration of a Data Domain system are as follows:

Procedure

1. Install the Data Domain hardware, including a system console, as described in the EMC Data Domain Installation and Setup Guide, which shipped with your Data Domain system. The Installation and Setup Guide provides instructions for installing your Data Domain system, connecting it to an administrative console, and powering it on. After you have completed installing and powering on your system, refer to this guide for additional information.

2. Define the Data Domain system information for your site as described in dd_t_prerequisites.

3. If you plan to use the Web-based Data Domain System Manager, determine how you will access it. You can enter one of the following in your Web browser’s address box:
   - A fully qualified domain name (for example, dd01.datadomain.com)
• A hostname (dd01)
• An IP address (10.5.50.5)

4. Perform the initial software configuration using one of the Configuration Wizards. See the Initial Configuration chapter.

5. If you changed the time, date, or time zone, reboot the Data Domain system.

6. Test the network connections.

7. If using the NFS protocol, mount directories for NFS-based backup servers and configure the backup software.

8. If using the CIFS protocol, when you connect from CIFS servers, set up user accounts and authentication on the CIFS server and set up backup software.

9. If using VTL, configure backup software for VTL data access and then set up the Data Domain system to use VTL (see the EMC Data Domain Operating System Administration Guide).

10. If using EMC DD Boost, configure backup software for EMC DD Boost for OpenStorage data access and the Data Domain system to use EMC DD Boost (see the EMC Data Domain Boost for OpenStorage Administration Guide).

11. Implement optional additional system configuration, such as giving access to additional backup servers and adding users to the email list that reports system problems.
CHAPTER 2

Initial Configuration

This chapter covers the following topics:

- Logging In ............................................................................................................. 16
- Using the System Manager’s Configuration Wizard ............................................. 16
- Rebooting the Data Domain System .................................................................... 20
- Using the CLI Configuration Wizard ................................................................... 21
Logging In

After you first log into the Data Domain system following the instructions given in your Installation and Setup Guide, you can use the Data Domain System Manager Wizard for configuration. If you choose not to use it, then the CLI Configuration Wizard is run.

**Note**

You must assign an IP address to a Data Domain system in order for it to access the System Manager. See your Installation and Setup Guide for more information.

You can use either wizard to configure the DD OS for the first time. The wizards configure what is needed for a basic system setup.

- **Data Domain System Manager Wizard**
  The Data Domain System Manager is a browser-based graphical user interface, available through Ethernet connections. Its Configuration Wizard is similar in content to the CLI-based Configuration Wizard, but provides a graphical interface with additional configuration options.

- **Command-Line Interface (CLI) Wizard**
  A command set that performs all system functions is available to users at the Command-Line Interface (CLI). Commands configure system settings and provide displays of system hardware status, feature configuration, and operation. The command-line interface is available through a serial console when a keyboard and monitor are directly attached to the Data Domain system, or remotely through an Ethernet connection using SSH or Telnet.

  After you configure the Data Domain system, you need to complete several post-configuration tasks, which are discussed in Post-Configuration Setup on page 27.

**Note**

- After the initial configuration, you can use either wizard to change or update the configuration. You must assign an IP address before you can use the System Manager.

- When configuring a Data Domain system as part of a Replicator pair, follow the same configuration steps as for a single system. If IPv6 addresses need to be configured for replication, use the CLI because Data Domain System Manager does not support the setting of IPv6 addresses.

Using the System Manager’s Configuration Wizard

Open your Web browser and enter your Data Domain system’s IP address in the browser’s address text box. Wait for the Data Domain System Manager to display the login screen. Enter your user name and password, and click Login.

The configuration modules are listed in the left pane. When one of the modules is selected, its details are shown in the main pane. You have the option of configuring or not configuring any module. You must start at the first module Licenses, however, and either configure or skip every module in order, ending with VTL Protocol.
Move through the modules using the Yes, No, Next, and Back buttons. Follow the instructions on the screen. To complete a module, gather the necessary data to enter. See Obtain this Information Before You Start on page 10. Also see the next table.

You can use the Quit button to exit the wizard. For help information, click the question mark in a dialog box.

After completing the Configuration Wizard:

- If you changed the date, time, or time zone, reboot the Data Domain system. See Rebooting the Data Domain System on page 20.
- Complete the post-configuration tasks discussed in Post-Configuration Setup on page 27.

**Note**

You can return to this wizard to reconfigure any modules from within the Data Domain System Manager. Click the Maintenance > System tab and select Launch Configuration Wizard from the More Tasks menu. See the EMC Data Domain Operating System Administration Guide for more information.

**Table 2** Data Domain System Manager Configuration Wizard Modules

<table>
<thead>
<tr>
<th>Modules</th>
<th>Information to be Entered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licenses</td>
<td>Your purchased license keys.</td>
</tr>
</tbody>
</table>
| Network | - General: Either use DHCP or manually enter the hostname, domain name, and gateway IP address.  
- Interfaces: Configure ports by using DHCP, or enter an IP address and netmask. |

**Note**

Select DHCP’s Enabled checkbox to enable the interface. When the interface is disabled, its settings cannot be changed.

- DNS information: DHCP or select an existing DNS IP address, or enter the DNS IP address.
Table 2 Data Domain System Manager Configuration Wizard Modules (continued)

<table>
<thead>
<tr>
<th>Modules</th>
<th>Information to be Entered</th>
</tr>
</thead>
<tbody>
<tr>
<td>File System (DD Extended Retention and non-DD Extended Retention versions)</td>
<td>For all file systems: Enable the file system after creation. For DD Extended Retention systems:</td>
</tr>
<tr>
<td></td>
<td>• Select whether or not to create a file system that supports Data Movement features and very large capacity.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Be sure that you want to create this kind of file system because it cannot be undone.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Configure Enclosures shows the available storage for the Retention Tier, formerly the Archive Tier. Select one or more available storage IDs and choose Retention (or Archive) as the tier configuration. Click the Add to Tier button, and click Next.</td>
</tr>
<tr>
<td></td>
<td>• Select the size of the first Retention (Archive) Unit.</td>
</tr>
<tr>
<td></td>
<td>• Select Enable the file system after creation.</td>
</tr>
<tr>
<td>System Settings</td>
<td>Set up the following to ensure that autosupport (ASUPs) and alert emails from your system are sent to Data Domain.</td>
</tr>
<tr>
<td></td>
<td>• Enter a password and email address for the Administrator. The email address is the address of the administrator who is to receive system emails, such as alerts and autosupport. Select all email options—to send alert notification, daily summaries, and autosupport.</td>
</tr>
<tr>
<td></td>
<td>• Mail Server. The name of the mail server used to send outgoing alert and autosupport emails to recipients.</td>
</tr>
<tr>
<td></td>
<td>Recipients are subscribers to groups. A group named default is created with the email address of two subscribers: the administrator and <a href="mailto:autosupport-alert@autosupport.datadomain.com">autosupport-alert@autosupport.datadomain.com</a>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>• Verify that the Send Alert Notification Emails to Data Domain is selected.</td>
</tr>
<tr>
<td></td>
<td>• Verify that the Send Vendor Support Notification Emails to Data Domain is selected.</td>
</tr>
<tr>
<td></td>
<td>• System Location. For your information only.</td>
</tr>
<tr>
<td></td>
<td>Review the Summary page carefully. The default address for alerts and autosupport emails to Data Domain is autosupport-alert @autosupport.datadomain.com.</td>
</tr>
</tbody>
</table>
### Table 2 Data Domain System Manager Configuration Wizard Modules (continued)

<table>
<thead>
<tr>
<th>Modules</th>
<th>Information to be Entered</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CIFS Protocol</strong></td>
<td>The Vendor email is listed as Sending. The vendor email address, which cannot be changed, is autosupport @autosupport.datadomain.com.</td>
</tr>
<tr>
<td></td>
<td>Workgroup: CIFS server name, if not using the default. Active Directory: Full realm name for the system, and a Domain Joining Credential user name and password.</td>
</tr>
<tr>
<td></td>
<td>Optionally, Organizational Unit name, if not using the default. Share name and directory path.</td>
</tr>
<tr>
<td></td>
<td>Client name, if not using the default.</td>
</tr>
<tr>
<td><strong>NFS Protocol</strong></td>
<td>Pathname for the export. NFS client server name to be added to /backup, if not using an existing client. Select NFS options for the client.</td>
</tr>
</tbody>
</table>

**Note**

These clients receive the default permissions, which are read and write permissions, root squashing turned off, mapping of all user requests to the anonymous UID/GID turned off, and secure.

| **EMC DD Boost Protocol** | • Either select an existing user, or add a new user by entering a user name and password.                                                              |
|                          | • Select the new user’s roles. See “User Roles” on page 27.                                                                                          |
|                          | • Optionally, change the Storage Unit Name in the text box.                                                                                          |
|                          | • If EMC DD Boost is to be supported over Fibre Channel transport, select the option to configure it.                                                   |
|                          | • Create an Access Group. Enter a unique name. Duplicate access groups are not supported.                                                          |
|                          | • Select one or more initiators. Optionally, replace the initiator name by entering a new one.                                                         |

**Note**

An initiator is a backup client that connects to the system for the purpose of reading and writing data using the Fibre Channel protocol. A specific initiator can support EMC DD Boost over FC or VTL, but not both.

The devices to be used are listed. They are available on all endpoints. An endpoint is the logical target on the Data Domain system to which the initiator connects.
Table 2 Data Domain System Manager Configuration Wizard Modules (continued)

<table>
<thead>
<tr>
<th>Modules</th>
<th>Information to be Entered</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTL Protocol</td>
<td>- Library name, number of drives, drive model, number of slots and CAPs, changer model name, starting barcode, and, optionally, tape capacity.</td>
</tr>
<tr>
<td></td>
<td>- Create an Access Group. Enter a unique name. Duplicate access groups are not supported.</td>
</tr>
<tr>
<td></td>
<td>- Select one or more initiators. Optionally, replace the initiator name by entering a new one.</td>
</tr>
</tbody>
</table>

**Note**

An initiator is a backup client that connects to the system for the purpose of reading and writing data using the Fibre Channel protocol. A specific initiator can support EMC DD Boost over FC or VTL, but not both.

The devices (drives and changer) to be used are listed. These are available on all endpoints. An endpoint is the logical target on the Data Domain system to which the initiator connects.

**User Roles**

A user can be assigned one of the following user roles:

- **Admin role**: Allows one to administer, that is, configure and monitor, the entire Data Domain system.
- **User role**: Allows one to monitor Data Domain systems and perform the fastcopy operation.
- **Security role**: In addition to the user role privileges, allows one to set up security-officer configurations and manage other security-officer operators.
- **Backup-operator role**: In addition to the user role privileges, allows one to create snapshots, import and export tapes to a VTL library and move tapes within a VTL library.
- **Data-access role**: Intended for EMC DD Boost authentication, an operator with this role cannot monitor or configure a Data Domain system.

**Rebooting the Data Domain System**

If you changed the date, time, or time zone during the initial configuration, reboot the Data Domain system. Otherwise, rebooting the system is not necessary.

**Procedure**

1. Select the Data Domain system to be rebooted in the System Manager’s Navigational pane.
2. Click **Maintenance > System**.
3. From the **More Tasks** menu select **Reboot System**.
4. Click **OK** at the Reboot System confirmation dialog box.
Using the CLI Configuration Wizard

About the CLI

The *EMC DD OS Command Reference Guide* provides information for using the commands to accomplish specific administration tasks.

Each command also has an online help page that gives the complete command syntax. Help pages are available at the CLI using the `help` command.

Any Data Domain system command that accepts a list (such as a list of IP addresses) accepts entries separated by commas, by spaces, or both.

The Tab key can be used:

- to complete a command entry when that entry is unique. Tab completion is supported for all keywords. For example, entering `systab` displays the command `system show stats`.
- to show next available option (if no characters are entered before pressing the Tab key)
- to show all the partial matched tokens or completes the entry if it is unique (when characters are entered before pressing the Tab key).

**Note**

After configuring the Data Domain system, reboot it only if you have changed the time zone. Use the `system reboot` command to shut down and reboot the system. This command automatically performs an orderly shutdown of file system processes.

Log Into the System Using the CLI

After performing the initial configuration, you can access the system to work with the CLI using one of these methods:

- From a serial console, use the communication settings 9600 baud, 8 data bits, no parity, and 1 stop bit.
- If your system includes a directly attached keyboard and monitor, log into the Data Domain system at the login prompt.
- From a remote machine over an Ethernet connection, use SSH to connect to the Data Domain system. Use the following command (with the hostname you chose for the Data Domain system at initial configuration) and provide the sysadmin password.

```bash
# ssh -l sysadmin hostname
Data Domain OS 5.4.0.0-19899
Password:
```

Find Online Help for Commands

There are several ways to find help for commands:

- To list Data Domain system commands, enter a question mark (?) or the command `help` at the prompt.
- To list the options for a particular command, enter the command with no options at the prompt.
To find a keyword used in a command option when you do not remember which command to use, enter a question mark (?) or the help command followed by the keyword. For example, the question mark followed by the keyword password displays all Data Domain system command options that include password. If the keyword matches a command, such as net, then the command explanation appears.

To display a detailed explanation of a particular command, enter the help command followed by a command name.

Use these help-related keyboard shortcuts:
- Up and down arrow keys to move through a displayed command
- The q key to exit
- A slash character (/) and a pattern to search for lines of particular interest. Matches are highlighted.

Using the CLI Configuration Wizard

If you do not choose to use the Data Domain System Manager Configuration Wizard for the initial configuration, use the CLI Configuration Wizard. To invoke the CLI Configuration Wizard after the initial setup, use the config setup command.

A description of each module follows.

Licenses

All licensed are installed at the factory, and a printed copy of the licenses is included with the packing slip.

To activate licensed features installed on your system, enter a valid license key. Enter the license characters, including dashes, for each feature you have licensed. For example, enter ABCD-ABCD-ABCD-ABCD

If you have not licensed a category, make no entry.

Network

Configure the Network

Procedure
1. Enter the Data Domain system’s hostname, which is a fully qualified name that includes the domain name. For example, enter dd01.xyz.com.

2. Enter a domain name, such as corporation.com, for use by the DNS, or accept the domain name that is part of the hostname. For example, enter xyz.com for the hostname dd01.xyz.com.

Configure Ethernet Interfaces (Ports)

Procedure
1. To enable the port, either use DHCP or assign a static IP address and netmask. If no address is to be assigned to the port, use the command: net config ifname up.
2. Select whether or not to use DHCP on the port.

If you are configuring the system using an Ethernet interface and you choose not to use DHCP, the Ethernet connection is lost when you complete the configuration.

If you have already set up DHCP for one or more Data Domain system Ethernet interfaces, the IP address and netmask prompts display the values given to the Data Domain system from a DHCP server. Press Enter to accept these values.

3. If DHCP is not configured on a port, enter the IP address and the netmask for the port.

4. If any port is not using DHCP, specify an IP address for a default routing gateway.

5. If no network port is configured to use DHCP, or DHCP is not configured to provide the DNS servers, you can specify one, two, or three DNS servers to resolve hostnames with IP addresses. Do one of the following:
   - Enter the server name or names, separating items in the list with either a comma or a space.
   - Choose to enter no servers by pressing the Enter key. In this case, use the `net hosts` command, which is described in the *EMC Data Domain Operating System Command Reference Guide*, to inform the Data Domain system of IP addresses for hostnames.

6. Press Enter.

7. If you have additional Ethernet ports, set them up as described above.

**Static Routing**

Static routes should be set if multiple interfaces contain the same IPv6 subnets, and the connections are being made to IPv6 addresses with this subnet. Normally, static routes are not needed with IPv4 addresses with the same subnet, such as for backups. There are cases in which static addresses may be required to allow connections to work, such as connections from the Data Domain system to remote systems.

**System Settings: Support and Alert Emails**

You must set up the following to ensure that support (ASUPs) and alert emails from your system are sent to Data Domain.

Enter the following information:

- **Admin Host**
  (Required) Enter a hostname that will have administrative access to the Data Domain system. When you log into this host via the internet or intranet, you can view system logs. The hostname can be a fully qualified domain name, a simple hostname, or an IP address. The host is added to all administrative access lists and is set up as an NFS client for both the `/backup` and `/ddvar` directories.

- **Admin Email**
  (Required) Enter the email address or a group alias that is to receive email from the Data Domain system. By default, the Data Domain system email list includes an address for the Data Domain Support group.

  The system uses the email address as the sender of alert and autosupport email messages from this system, and as the recipient for these messages.
Note

- The autosupport feature sends a daily report to Data Domain Support that shows system identification information and consolidated output from Data Domain system commands and entries from various log files.
- Alerts occur whenever the system's Restore Protection Manager discovers a problem with software or a monitored hardware component. The alert command manages the alerts history file and who receives email notification for system alerts.
- For more information about autosupport and alerts, see the *EMC DD OS Administration Guide*.

- System Location
Enter a physical location that identifies this system for use in autosupport emails. For example, enter **Bldg4-rack10**. The alerts and autosupport reports display the location.
- SMTP Mail Server
Enter the name of a local SMTP (mail) server that relays Data Domain system emails. If the server is an Exchange server, be sure that SMTP is enabled.
- Time Zone
The system date has already been set. Changing the time zone requires that you reboot the Data Domain system.

Using the tables in *Time Zones on page 45*, determine your local time zone. The default time zone for each Data Domain system is **US/Pacific**.

Note
Each time zone consists of two parts, which are separated with a slash (/).

- Network Time Service (NTP) Servers
The default is to enable NTP and to use multicast for NTP.

If DHCP is set up, do the following only if the DHCP server is not configured to provide the NTP servers:

To allow the Data Domain system to use one or more Network Time Service (NTP) servers to synchronize its clock, enter their IP addresses or server names, separated by commas.

CIFS Protocol

Note
A single Data Domain system can receive backups from both CIFS and NFS clients only if separate directories or MTrees are used for each protocol. Do not mix CIFS and NFS data in the same directory.

The *backup* directory is the destination directory on the Data Domain system for compressed backup server data.
NFS Protocol

Note
A single Data Domain system can receive backups from both CIFS and NFS clients as long as separate directories are used for each. Do not mix CIFS and NFS data in the same directory.

The backup servers that can access the Data Domain system through NFS are the NFS clients of the system’s backup file system. The /backup directory is the destination directory on the Data Domain system for compressed backup server data.

EMC DD Boost Protocol

For the initial setup, you are prompted to enter your EMC DD Boost user name, which can be any EMC DD Boost user name. This name is used for EMC DD Boost authentication only. When prompted, save your settings.

After initial configuration, you typically create new storage units, display existing storage units, and set storage unit options using the ddboost command options.

VTL Module

Follow these steps to configure VTL using the CLI Configuration Wizard’s VTL module. Ranges for all of the values you are to enter are shown, such as 1 - 32 characters for the VTL library’s name. For more information about configuring VTL, see the DD OS Administration Guide.

Procedure
1. You are prompted to create a VTL library by entering an appropriate name.
2. Enter the library’s emulation (changer) model: L180, RESTORER-L180, or TS3500.
   Two other models, the i2000 and TS3200 are supported, but these models must be set up using either the DD System Manager or the command vtl group add.
3. As prompted, enter the number of slots and the number of CAPS (Cartridge Access Ports).
4. Enter the drive model and the number of drives. The model options are IBM-LTO-1, IBM-LTO-2, or IBM-LTO-3.
   The drives HP-LTO-3, HP-LTO-4, and IBM-LTO-4 are also supported, but you must add them using either the DD System Manager or the command vtl drive add.
5. Define the tape parameters: barcode and capacity.
   The eight-character barcode must start with six numeric or upper-case alphabetic characters (from the set {0-9, A-Z}) and end in a two-character code for the supported tape type; for example, A99000LA. For tape capacity, enter 0 to have the value derived from the barcode.

<table>
<thead>
<tr>
<th>Tape Code</th>
<th>Tape Capacity in GiB</th>
<th>Tape Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>L1</td>
<td>100</td>
<td>LTO-1</td>
</tr>
<tr>
<td>L2</td>
<td>200</td>
<td>LTO-2</td>
</tr>
<tr>
<td>L3</td>
<td>400</td>
<td>LTO-3</td>
</tr>
<tr>
<td>L4</td>
<td>800</td>
<td>LTO-4</td>
</tr>
</tbody>
</table>
### Initial Configuration

<table>
<thead>
<tr>
<th>Tape Code</th>
<th>Tape Capacity in GiB</th>
<th>Tape Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>LA</td>
<td>50</td>
<td>LT0-1</td>
</tr>
<tr>
<td>LB</td>
<td>30</td>
<td>LT0-1</td>
</tr>
<tr>
<td>LC</td>
<td>10</td>
<td>LT0-1</td>
</tr>
</tbody>
</table>

6. Enter a descriptive name for a VTL access group.

VTL Access groups define logical groupings, which include initiators and targets. An access group is logically equivalent to LUN masking.

7. Select yes at the next prompt to add VTL initiators to the previously created group. You must know the initiator's name to enter it; for example: `pe2950_hba_zone_01`. After the initial configuration assign an alias to an initiator using the `vtl initiator set alias` command.

8. Continue to add initiators until all are included in the access group.

After adding initiators, the pending settings for the configured VTL are displayed.

<table>
<thead>
<tr>
<th>Pending Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Library name</td>
</tr>
<tr>
<td>Changer model</td>
</tr>
<tr>
<td>Slots</td>
</tr>
<tr>
<td>CAPs</td>
</tr>
<tr>
<td>Drive Model</td>
</tr>
<tr>
<td>Drives</td>
</tr>
<tr>
<td>Barcode</td>
</tr>
<tr>
<td>Capacity</td>
</tr>
<tr>
<td>Group name</td>
</tr>
<tr>
<td>Initiators</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

9. Review and save your settings.
CHAPTER 3

Post-Configuration Setup

After the initial configuration, perform these post-configuration tasks, as appropriate for your installation. This chapter covers the following topics:

- Verify Support and Alert Emails ................................................................. 28
- Security and Firewalls (NFS and CIFS Access) ................................................. 29
- Verifying Network Connections ................................................................. 29
- About the /ddvar Directory (NFS and CIFS Clients) .................................. 29
- Configuring the Data Domain System for Data Access .......................... 29
Verify Support and Alert Emails

**Note**

Do not continue with the configuration until you verify that Data Domain can receive support and alert emails from your system. Do this whether you used the CLI or Data Domain System Manager Wizard for the initial setup.

**Procedure**

1. Assign an IP address to the Data Domain system using the CLI if you have not already done so.
2. Open your Web browser and enter your Data Domain system’s IP address in the browser’s address text box. Wait for the Data Domain System Manager to display the login screen.
3. Enter your user name and password, and click **Login**.
4. Do one of the following:
   - If you used the Data Domain System Manager Configuration Wizard, go to Step 5.
   - If you used the CLI Configuration Wizard, do the following:
     a. Click the **Maintenance > System** tab and select **Launch Configuration Wizard** from the More Tasks menu.
     b. Click through each of the modules by entering **No** or **Next** until you reach **System Settings**. Click **Yes** to configure system settings.
     c. Verify the Administrator information is correct. Click **Next**.
     d. The Email information in the Email/Location section must be correct. Verify the name of the mail server to be used to send outgoing Alert and Autosupport emails to recipients.
     e. Verify that **Send Alert Notification Emails to Data Domain** is selected.
     f. Verify that the **Send Vendor Support Notification Emails to Data Domain** is selected. The address, which cannot be changed, is autosupport@autosupport.datadomain.com. This notification status is enabled by default. The mail server location is for your information only.
     g. Click **Next** and verify that the information you entered is correct in the Summary. If not, go back to the sections that need changing and edit them.
     h. After approving the updated Summary, click **Submit**.
     i. Click **Next** to exit each of the remaining modules. Exit the Configuration Wizard.
5. Go to **Maintenance > Support > Autosupport**. In the Vendor Support area, verify that the Notification Status for vendors is Enabled. You cannot change the email address.
6. Go to **Status > Alerts > Notification**. In the **Alerts** area, verify that **default** is selected as a group. Verify that the **Subscribers Email List** contains the administrator and autosupport-alert@autosupport.datadomain.com addresses.

**Note**

You can create other groups; add, modify, and delete email subscribers to groups; and set class attributes. Class attributes refer to the name of a class, such as Hardware or File System. You set the severity of ranking, such as Warning or Critical, that is to trigger an alert for each class attribute. For more information, see the section that discusses the Notification View in the *EMC Data Domain Operating System Administration Guide*. 
Security and Firewalls (NFS and CIFS Access)

The firewall should be configured so that only required and trusted clients have access to the Data Domain system.

Please consult with your EMC technical support professional for instructions on setting up NFS and CIFS access through a firewall.

By default, anonymous users from known CIFS clients have access to the Data Domain system. For security purposes, change this option from disabled (the default) to enabled:

```bash
# cifs option set restrict-anonymous enabled
```

Verifying Network Connections

Test both directions for each Data Domain interface on which traffic is expected for connectivity.

Issue the `ping` command from a remote system to the hostname and issue the `ping` command from the host name to a remote system. If a port is on a private network or is directly attached, the remote system must be on the same private network, or directly attached, for you to test it.

About the /ddvar Directory (NFS and CIFS Clients)

The `/ddvar` directory contains Data Domain system core and log files. NFS and CIFS clients that need administrative access should be able to access this directory.

The `/ddvar` directory has the following subdirectories:

- `README`
- `certificates`
- `core`, which is the default destination for core files created by the system.
- `log`, which is the destination for all system log files. As of DD OS 5.3, log messages from CIFS subsystem are logged only in `debug/cifs/cifs.log`. Examine this log file for CIFS issues.
- `traces`, which is the destination for execution traces used in debugging performance issues.
- `releases`, which is the default destination for operating system upgrades (the RPM files) that are downloaded from the Support Web site.
- `snmp`, which is the location of the SNMP (Simple Network Management Protocol) MIB (Management Information Base).
- `support`, which is the location for logs and autosupport files. Access this directory to send autosupport files for Support, and for images for upgrading the Data Domain system. You can enable a CIFS share or NFS export to this location, as well as use FTP.

Create a CIFS Share to /ddvar

Specify clients allowed to access a Data Domain system’s `/ddvar` directory:

```bash
# cifs add /ddvar client-list
```

Configuring the Data Domain System for Data Access

After completing the Configuration Wizard, you need to configure clients that access the Data Domain system.
Procedure
2. In the Navigation pane, click Documentation.
3. On the Documentation page, click Integration Documentation.
4. Select the vendor for the client system’s operating system, such as Sun or Microsoft, and click OK.
5. Select the appropriate tuning document, such as the Solaris System Tuning or the CIFS Tuning Guide.
This chapter describes some additional configuration procedures that are performed once the initial configuration with the Configuration Wizard is complete. This chapter covers the following major topics:

- Changing the Timeout on CIFS Backup Servers .......................................................... 32
- Advanced Network Configuration .............................................................................. 32
- Configuring SNMP on a Data Domain System ............................................................ 38
- Configuring SOL for IPMI ......................................................................................... 39
- Configuring Encryption for Data at Rest ................................................................... 39
- Optional Configuration Procedures .......................................................................... 39
Changing the Timeout on CIFS Backup Servers

If internal activities on a Data Domain system take longer than the default CIFS timeout, the media server displays an error message that says the network name no longer exists. On all CIFS backup servers that use a Data Domain system, change the `SESSTIMEOUT` value from the default of 45 (seconds) to 300 (five minutes).

Change the Default Timeout Value

Procedure

1. Open the Registry Editor on the Windows machine. Go to **Start** > **Run** and type this in the Open text box:
   ```
   REGEDT32
   ```
2. Click **OK**.
3. Expand the **My Computer** node in the left pane.
4. Expand **HKEY_LOCAL_MACHINE** and continue to expand nodes in the directory tree until you reach the parameters menu from this path: **SYSTEM** > **CurrentControlSet** > **Services** > **lanmanworkstation** > **parameters**.
5. If there is a **SESSTIMEOUT** key, it is located in the name list in the right pane. If there is no such key, right-click within an empty space in the right pane, select **New** > **Key**, and name the new key **SESSTIMEOUT**, using all caps.
6. Double-click the **SESSTIMEOUT** key and set its value to 300.

Advanced Network Configuration

The following additional advanced network features can be configured on the Data Domain system:

- **Ethernet Failover**
  
  You can configure multiple network interfaces on a Data Domain system to function as a single virtual interface. Should a network interface configured as part of a virtual interface fail, network activity switches to another port. Ethernet failover provides improved network stability.

- **Link Aggregation**
  
  With link aggregation, multiple physical Ethernet network ports can be used in parallel, which increases the link speed and also provides a reduced performance failover capability over that of a single port. See the *EMC DD OS Administration Guide* and *EMC DD OS Command Reference Guide* for details.

- **VLAN Tagging**
  
  You can set an interface on the Data Domain system to support multiple IEEE 802.1Q VLANs, with an interface configured with a distinctive VLAN IP address. The switch that connects to the interface must also be configured to send data from multiple VLANs to the Data Domain system, using the proper VLAN encapsulation, as specified by the 802.1Q protocol.

About the Ethernet Interface Ports

The Ethernet port- naming convention used for all Data Domain systems shipped prior to DD OS 4.9 included only a number for each port without regard to physical location of that port (for example, eth0 to eth5). Starting with new systems shipped with DD OS 4.9, the Ethernet Interface-naming scheme references both a PCI slot location and a specific...
port on the NIC (for example, ethSlotPort, where Slot is the Ethernet card location in the
system, and Port is the port, for example, a or b).

On EMC platforms, built-in Ethernet ports use slot M (Motherboard), and IO card
numbering starts at zero.

To obtain information about the ports on your Data Domain system, use the command
net show hardware.

Although Ethernet ports are typically configured in pairs, more than two ports can be
configured as a virtual interface. Each physical Ethernet port, however, can be a part of
only one virtual interface.

Create a Virtual Interface

Virtual interfaces used for failover or link aggregation must be created from pairs that are
supported for the kind of interface you are creating.

- The maximum number of virtual interfaces is limited to the number of physical ports
  on the system. Data Domain recommends a maximum of two virtual interfaces per
  Data Domain system.
- In most cases, virtual interfaces should be created from identical physical interfaces,
  that is, all copper or all fiber, 1 GbE to 1 GbE, and NIC to NIC. Two exceptions are that
  you can mix 1 GbE optical to 1 GbE copper and a copper port on the motherboard to a
  copper port on a NIC.
- A VLAN interface cannot be created on a failover interface consisting of Chelsio 10
  GbE interfaces.
- All physical interfaces associated with a virtual interface must be on the same subnet
  and on the same LAN. Legacy cards must be on the same card for a 10 GbE virtual
  interface. Network switches used by a virtual interface must be on the same subnet.

Follow these steps to create a virtual interface:

Procedure

1. Use the net createl command. Enter: 
   #net create virtual vethx
   
   where x is the variable for the virtual name (and this exact format is required). The
   variable consists of decimal or hexadecimal numbers (0-9 and aA-fF) that serve as an
   unique identifier for the virtual interface.

2. Use the net config command to assign the virtual interface (ifname) an IP address
   and an optional netmask. Enter: 
   #net config ifname ipaddr netmask netmask

   **Note**

   DHCP is not supported for virtual interfaces, so the IP address must be assigned.

Configure Failover

To configure failover:

**Note**

The on-board port ethMa is to be used only for maintenance and should not be bonded
with optional card ports.
Procedure

1. Create a virtual interface and assign it an IP address. See Create a Virtual Interface on page 33 for instructions.

2. Disable each of the Ethernet ports *ifname* that are to be part of the virtual interface by entering the following command, for each port:

   ```
   # net disable ifname
   ```

   where *ifname* is the port name. For example:

   ```
   # net disable eth4a
   # net disable eth4b
   ```

3. Configure failover with the virtual interface name you created in step 1 and add the designated network interfaces. To assign one of the network interfaces as the primary failover interface, use the optional `primary` parameter.

   Enter:

   ```
   # net failover add virtual-ifname interfaces ifname-list [primary ifname]
   ```

   For example, to configure failover for the virtual interface named `veth1` using the physical ports `eth4a` and `eth4b`, and to assign `eth4a` as the primary port, enter:

   ```
   # net failover add veth1 interfaces eth4a eth4b primary eth4a
   ```

   This output displays:

   ```
   Interfaces for veth1: eth4a, eth4b
   ```

4. Assign an IP address and netmask to the new interface:

   ```
   # net config ifname ipaddr netmask mask
   ```

   where *ifname* is the name of the interface (`veth1` in this example) and `mask` is the corresponding netmask.

5. Verify that the interface has been configured by entering:

   ```
   # net failover show
   ```

   The hardware address and configured interfaces (eth4a, eth4b) for the interface named `veth1` are displayed.

6. (Optional) To add another physical interface, such as `eth5a`, to the virtual interface, enter:

   ```
   # net failover add veth1 interfaces eth5a
   ```

   This output displays: `Interfaces for veth1: eth4a, eth4b, eth5a`

7. (Optional) To change the physical interface assigned as the primary failover interface, enter:

   ```
   # net failover modify virtual-ifname primary {ifname | none}
   ```

Configure Link Aggregation

The `net aggregate` command enables a virtual interface for link aggregation with the specified physical interfaces using one of these aggregation modes. You need to specify an aggregate mode first; there is no default aggregate mode.

**DD OS 5.4 Limitation:** Link aggregation is not supported for the DD2500’s on-board 10G Base-T interfaces, which are ethMe and ethMf.
Do not use the Akula NIC for customer data.

Select the mode that is compatible with the switch in use:

- **roundrobin**
  Transmits packets in sequential order from the first available link through the last in the aggregated group.

- **xor-L2**
  Route transmit packets based on static balanced mode aggregation with an XOR hash of Layer 2 (inbound and outbound MAC addresses).

- **xor-L2L3**
  Route transmit packets based on static balanced mode aggregation with an XOR hash of Layer 2 (inbound and outbound MAC addresses) and Layer 3 (inbound and outbound IP addresses).

- **xor-L3L4**
  Route transmit packets based on static balanced mode aggregation with an XOR hash of Layer 3 (inbound and outbound IP address) and Layer 4 (inbound and outbound port numbers).

- **lacp**
  A link aggregation mode based on the Link Aggregation Control Protocol (IEEE 802.3ad).

  Communicates with the other end to coordinate which links within the bond are available. When this mode is selected, both ends must be configured with lacp.

Some considerations for configuring link aggregation:

- Two or more Ethernet ports can be configured as interfaces for link aggregation.
- A physical port cannot already be configured for VLAN.
- All physical ports in the link aggregation group must be connected to the same switch, unless the switch can support the sharing of EtherChannel information.

To configure link aggregation:

**Procedure**

1. Create a virtual interface and assign it an IP address. See Create a Virtual Interface on page 33 for instructions.
2. Disable each of the physical ports that you plan to use as aggregation interfaces.
   Enter: 
   
   ```
   net disable ifname
   ```
   where ifname is the port name. For example, for eth2a and eth2b:
   
   ```
   net disable eth2a
   ```
   ```
   net disable eth2b
   ```

3. Create an aggregate virtual interface by specifying the physical ports and mode (the mode must be specified the first time). Choose the mode that is compatible with the requirements of the switch to which the ports are directly attached. Enter:
   
   ```
   net aggregate add virtual-ifname mode {roundrobin | xor-L2 | xor-L2L3} interfaces physical-ifname-list
   ```
   For example, to enable link aggregation on virtual interface veth1 to physical interfaces eth1a and eth2a in mode xor-L2, enter:
   
   ```
   net aggregate add veth1 mode xor-L2 interfaces eth1a eth2a
   ```

4. Assign an IP address and netmask to the new interface using this command:  
   
   ```
   net config ifname ipaddr netmask
   ```
where `ifname` is the name of the interface, which is `veth1` in this example, `ipaddr` is the interface's IP address, and `mask` is the netmask.

5. To verify that the interface has been created, enter: `

```bash
# net aggregate show
```

The output displays the name of the virtual interface, its hardware address, aggregation mode, and the ports that comprise the virtual interface.

**Configure VLAN Tagging**

To configure VLAN tagging:

**Procedure**

1. Configure the switch port that connects to the interface that is to receive and send VLAN traffic from the Data Domain interface. See the switch documentation for details on the configuration.

2. On the Data Domain system, enable the interface that you plan to use as the VLAN interface, such as `eth5b`, by entering: `

```bash
# net config eth5b up
```

3. Create the VLAN interface using either a physical port or a configured virtual port (to create the virtual port, see Create a Virtual Interface on page 33. The range for `vlan-id` is between 1 and 4094 inclusive: `

```bash
# net create interface {physical-ifname | virtual-ifname} vlan vlan-id
```

For example, to create a VLAN interface on a physical interface `eth5b`, enter: `

```bash
# net create interface eth5b vlan 1
```

A VLAN interface named `eth5b.1` is created.

4. Assign an IP address and netmask to the new interface using this command: `

```bash
# net config ifname ipaddr netmask
```

where `ifname` is the name of the interface, which is `eth5b.1` in this example, `ipaddr` is the interface's IP address, and `mask` is the corresponding netmask.

**Note**

DHCP cannot be used to assign an IP address to a VLAN.

5. To verify that the interface has been created, enter: `

```bash
# net show settings
```
The following information displays:

<table>
<thead>
<tr>
<th>Port Enabled</th>
<th>DHCP</th>
<th>IP Address</th>
<th>Netmask</th>
<th>Type</th>
<th>Additional Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth5b1</td>
<td>yes</td>
<td>yes</td>
<td>192.168.8.175*</td>
<td>255.255.252.0*</td>
<td>n/a</td>
</tr>
</tbody>
</table>

After you finish

For more information, see the *EMC Data Domain Operating System Command Reference Guide*.

**Additional Physical or Virtual Interface Configuration**

You can set the maximum transfer unit (MTU) size and configure duplex line usage and speed.

**Specify the MTU**

You can set the MTU size for a physical or virtual interface, or a vlan interface if the MTU size is less than or equal to the underlining base interface MTU value. Supported
maximum transfer unit size values range from 1500 to 9000. For 100 Base-T and gigabit networks, 1500 is the default.

**Note**

Although 9000 is the maximum size, to be backward compatible, the DD OS accepts up to 9014, but sets the value to 9000 when it is greater than 9000 and less than or equal to 9014.

Use the `default` option to return the setting to the default value.

**Note**

All of your network components need to support the size that you set. Incorrectly setting MTU affects system performance.

The minimum size for MTU is 350, except when the IP address is set to IPv6. In this case the minimum MTU is 1280.

Enter:

```
# net config ifname mtu {size | default}
```

where `ifname` is the name of the interface.

### Configure Duplex Line Use and Speed

To configure the duplex line use and speed for an interface, use one of these three options:

- Set the duplex line use for an interface to either half- or full-duplex and set its port line speed for 10, 100, or 1000 Base-T (gigabit).
- Have the network interface card automatically negotiate these settings for an interface.

**Note**

The following restrictions apply:

- Duplex line use and auto-negotiate do not apply to 10 GbE cards.
- A line speed of 1000 must have a full-duplex setting.

To set an interface’s duplex line use, enter: `# net config ifname duplex {full|half} speed {10 | 100 | 1000}`

For example, to set `veth1` to duplex with a speed of 100 Base-T, enter: `# net config veth1 duplex half speed 100`

### Set Auto-Negotiate for an Interface

**Procedure**

1. Enter: `# net config ifname autoneg`

For example, to set auto-negotiate for interface `eth1a`, enter:

```
# net config eth1a autoneg
```

### Routing Tables and Gateways

After you have configured the interface for failover, aggregation, or VLAN tagging, assigned an IP address, set the netmask, and enabled the interface, the interface is
automatically added to the routing table. The new entry should appear when you enter: 
route show table

The virtual interface is in the same subnet as the physical interface; therefore, the default gateway does not change.

Configuring SNMP on a Data Domain System

From an SNMP perspective, a Data Domain system is a read-only device with this exception—a remote machine can set the SNMP location, contact, and system name on a Data Domain system. To configure community strings, hosts, and other SNMP variables on the Data Domain system, use the `snmp` command.

With one or more trap hosts defined, a Data Domain system takes the additional action of sending alert messages as SNMP traps, even when the SNMP agent is disabled.

Display Configuration Commands
To view the current SNMP configuration, enter: 
```
# snmp show config
```

Add a Community String
As an administrator, enter one of these commands that enable access to a Data Domain system, either to add read/write (rw) or read-only (ro) permission:

```
# snmp add rw-community community-string-list [hosts host-list]
# snmp add ro-community community-string-list [hosts host-list]
```

For example, to add a community string of private with read/write permissions, enter: 
```
# snmp add rw-community private hosts host.datadomain.com
```

Enable SNMP
By default, SNMP is disabled on the Data Domain system. To enable SNMP, at least one read or read/write community string must be set before the `snmp enable` command is given.

As an administrator, enter:
```
# snmp enable
```

The default port that is opened when SNMP is enabled is port 161. Traps are sent to port 162.

Set the System Location
As an administrator, enter:
```
# snmp set sysLocation location
```

This command sets the system location as used in the SNMP MIB II system variable `sysLocation`. For example:
```
snmp set sysLocation bldg3-rm222
```

Set a System Contact
As an administrator, enter:
```
# snmp set sysContact contact
```

This command sets the system contact as used in the SNMP MIB II system variable `sysContac`. For example:
```
#snmp set sysContac bob-smith
```
The SNMP sysContact variable is not the same as that set using the `config set admin-email` command. If the SNMP variables are not set with the `snmp` commands, the variables default to the system values given as part of the `config set commands`.

Add a Trap Host
As an administrator, enter:

```
# snmp add trap-host host-name-list[:port[version {v2c | v3 }][community community | user]]
```

where `host` may be a hostname or an IP address. By default, port 162 is assigned, but you can specify another port. For example, to add a trap host `admin12`, enter:

```
# snmp add trap-host admin12 version v2c community public
```

This command adds a trap host to the list of machines that receive SNMP traps generated by the Data Domain system. With one or more trap hosts defined, alert messages are also sent as traps, even when the SNMP agent is disabled.

Configuring SOL for IPMI

You can use the Intelligent Platform Management Interface (IPMI) to power up, power down, or power cycle a Data Domain system in a remote location from a host Data Domain system, if both systems support this standard. The Serial-Over-LAN (SOL) feature of IPMI is used to view the serial output of a remote system's boot sequence. Instructions for configuring SOL for IPMI are included in the [EMC Data Domain Operating System Command Reference Guide](#).

Configuring Encryption for Data at Rest

The optional Encryption for Data at Rest feature encrypts all incoming data before writing it to the Data Domain system's physical storage media. The data is physically stored in an encrypted manner and cannot be accessed on the existing Data Domain system or in any other environment without first decrypting it.

---

**Note**

Optimally, the Encryption for Data at Rest feature should be configured when setting up your system. Data is encrypted only after the feature's configuration is complete, that is, any pre-existing data will not be encrypted.

To learn more about how the Encryption at Rest feature works, and to view configuration and management procedures, see the [EMC Data Domain Operating System Administration Guide](#).

Optional Configuration Procedures

You can perform the following tasks now or later. See the [EMC Data Domain Operating System Administration Guide](#) for more information.

- Add users
- Enable FTP, FTPS, SCP, and Telnet for data access
- Add remote hosts that can use FTP or Telnet
- Add email addresses to receive system reports
Additional Configuration
CHAPTER 5

Adding Expansion Shelves

This chapter covers the following topics:

- **Overview** .......................................................................................................................... 42
- **Add Enclosure Disks to the Volume** .................................................................................. 42
- **Disks Labeled Unknown Instead of Spare** ......................................................................... 43
- **Verify Shelf Installation** ..................................................................................................... 43
Overview

Install the new expansion shelf as described in the Data Domain Expansion Shelf Hardware Guide for your shelf model or models. The procedure described here, which adds shelves to the volume and creates RAID groups, applies only to adding a new expansion shelf to the active tier of a Data Domain system. For adding shelves to a system with the Extended Retention feature, see the appropriate Data Domain Expansion Shelf Hardware Guide and the EMC Data Domain Extended Retention Administration Guide.

The Data Domain system recognizes all data storage (system and attached shelves) as part of a single volume.

Mixing SAS and SATA disks within an enclosure is not supported, and mixing SAS and SATA disk enclosures on the same SAS chain is not supported.

<table>
<thead>
<tr>
<th>DD Platform</th>
<th>SAS Support</th>
<th>SATA Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>DD2500</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>DD4500</td>
<td>Headswap Only</td>
<td>Yes</td>
</tr>
<tr>
<td>All Other Models</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**CAUTION**

Do not remove a shelf that has been added unless you are prepared to lose all data in the volume. If a shelf is disconnected, the volume's file system is immediately disabled. To re-enable it, reconnect the shelf or transfer the shelf disks to another shelf chassis and connect the new chassis. If the data on a shelf is not available to the volume, the volume cannot be recovered. Unless the same disks are in the original shelf or in a new shelf chassis, the DD OS must be re-installed as directed by your contracted service provider or Data Domain's Support site (https://my.datadomain.com/).

Add Enclosure Disks to the Volume

Procedure

1. Use the following command: `# storage add [tier {active | archive}] {enclosure enclosure-id | dev disk-id [spindle-group 1-16 | disk enclosure-id disk-id]}` where `enclosure-id` is always 2 for the first added shelf and 3 for the second.

   **Note**
   
   The EMC Data Domain controller always has the enclosure-id of 1 (one).

2. When prompted, enter your sysadmin password.

3. (Optional) Add disks in another enclosure at this time using the above-mentioned `storage add` command.

4. Display the RAID groups for each shelf by entering: `storage show all`

   **Note**
   
   EMC ES30 shelves have one spare disk. ES20 shelves have two spare disks. The rest of the disks should report that they are available or spare disks.
Disks Labeled Unknown Instead of Spare

Procedure

1. Enter the `disk unfail` command for each unknown disk. For example, if the two disks 2.15 and 2.16 are labeled unknown, enter commands like these:

   # disk unfail 2.15
   # disk unfail 2.16

2. Verify the new state of the file system and disks by entering: `filesys status`

3. After a shelf has been added to the file system, you can view the total size, amount of space used, and available space for each file system resource, such as data, metadata, and index, by entering: `filesys show space`.

Verify Shelf Installation

Procedure

1. After installing the new shelves, check the status of the SAS HBA cards by entering: `disk port show summary`

   The output shows the port for each SAS connection, such as 3a and 4a, and the online status, which is offline. After the shelves have been connected, the same command also displays the connected enclosure IDs for each port, such as 2 and 3. The status changes to online.

2. Verify that the Data Domain system recognizes the shelves by entering: `enclosure show summary`

   This command shows each recognized enclosure ID, Data Domain system model number, serial number, and slot capacity, as well as state of the enclosure and information about the shelf's manufacturer.
Adding Expansion Shelves
APPENDIX A

Time Zones

This chapter covers the following topics:

◆ Time Zones Overview
◆ Africa
◆ America
◆ Antarctica
◆ Asia
◆ Atlantic
◆ Australia
◆ Brazil
◆ Canada
◆ Chile
◆ Etc
◆ Europe
◆ GMT
◆ Indian (Indian Ocean)
◆ Mexico
◆ Miscellaneous
◆ Pacific
◆ System V
◆ US (United States)
◆ Aliases
Time Zones Overview

Time zones are used when you initially configure your system to establish the location. Locate your time zone using the following tables. A time zone usually consists of two entries separated by a slash (/). The first entry is usually a continent, nation, or region such as Africa, the Pacific, or the United States. The second entry is usually the city within that area that is closest to you. There are also aliases for time zones and miscellaneous entries, such as GMT, Cuba, and Japan that are single entries.

Examples of time zones include:
- GMT+5
- Stockholm
- Pacific
- EasterIsland
- Japan

Africa

<table>
<thead>
<tr>
<th>City</th>
<th>City</th>
<th>City</th>
<th>City</th>
<th>City</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abidjan</td>
<td>Accra</td>
<td>Addis_Ababa</td>
<td>Algiers</td>
<td>Asmera</td>
</tr>
<tr>
<td>Bamako</td>
<td>Bangui</td>
<td>Banjul</td>
<td>Bissau</td>
<td>Blantyre</td>
</tr>
<tr>
<td>Brazzaville</td>
<td>Bujumbura</td>
<td>Cairo</td>
<td>Casablanca</td>
<td>Ceuta</td>
</tr>
<tr>
<td>Conakry</td>
<td>Dakar</td>
<td>Dar_es_Salaam</td>
<td>Djibouti</td>
<td>Douala</td>
</tr>
<tr>
<td>El_Aaiun</td>
<td>Freetown</td>
<td>Gaborone</td>
<td>Harare</td>
<td>Johannesburg</td>
</tr>
<tr>
<td>Kampala</td>
<td>Khartoum</td>
<td>Kigali</td>
<td>Kinshasa</td>
<td>Lagos</td>
</tr>
<tr>
<td>Libreville</td>
<td>Lome</td>
<td>Luanda</td>
<td>Lubumbashi</td>
<td>Lusaka</td>
</tr>
<tr>
<td>Malabo</td>
<td>Maputo</td>
<td>Maseru</td>
<td>Mbabane</td>
<td>Mogadishu</td>
</tr>
<tr>
<td>Monrovia</td>
<td>Nairobi</td>
<td>Ndjamena</td>
<td>Niamey</td>
<td>Nouakchott</td>
</tr>
<tr>
<td>Ouagadougou</td>
<td>Porto-Novot</td>
<td>Sao_Tome</td>
<td>Timbuktu</td>
<td>Tripoli</td>
</tr>
<tr>
<td>Tunis</td>
<td>Windhoek</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

America

<table>
<thead>
<tr>
<th>City</th>
<th>City</th>
<th>City</th>
<th>City</th>
<th>City</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adak</td>
<td>Anchorage</td>
<td>Anguilla</td>
<td>Antigua</td>
<td>Araguaina</td>
</tr>
<tr>
<td>Aruba</td>
<td>Asuncion</td>
<td>Atka</td>
<td>Barbados</td>
<td>Belem</td>
</tr>
<tr>
<td>Belize</td>
<td>Boa_Vista</td>
<td>Bogota</td>
<td>Boise</td>
<td>Buenos_Aires</td>
</tr>
<tr>
<td>Cambridge_Bay</td>
<td>Cancun</td>
<td>Caracas</td>
<td>Catamarca</td>
<td>Cayenne</td>
</tr>
<tr>
<td>Cayman</td>
<td>Chicago</td>
<td>Chihuahua</td>
<td>Cordoba</td>
<td>Costa_Rica</td>
</tr>
<tr>
<td>Cuiaba</td>
<td>Curacao</td>
<td>Danmarkshavn</td>
<td>Dawson</td>
<td>Dawson_Creek</td>
</tr>
<tr>
<td>Denver</td>
<td>Detroit</td>
<td>Dominica</td>
<td>Edmonton</td>
<td>Eirunepe</td>
</tr>
<tr>
<td>El_Salvador</td>
<td>Ensenada</td>
<td>Fortaleza</td>
<td>Fort_Wayne</td>
<td>Glace_Bay</td>
</tr>
<tr>
<td>Godthab</td>
<td>Goose_Bay</td>
<td>Grand_Turk</td>
<td>Grenada</td>
<td>Guadeloupe</td>
</tr>
<tr>
<td>Guatemala</td>
<td>Guayaquil</td>
<td>Guyana</td>
<td>Halifax</td>
<td>Havana</td>
</tr>
<tr>
<td>Hermosillo</td>
<td>Indiana/Indianapolis</td>
<td>Indiana/Knox</td>
<td>Indiana/Marengo</td>
<td>Indianapolis</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------</td>
<td>--------------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Indiana/Vevay</td>
<td>Inuvik</td>
<td>Iqaluit</td>
<td>Jamaica</td>
<td>Jujuy</td>
</tr>
<tr>
<td>Juneau</td>
<td>Kentucky/Louisville</td>
<td>Kentucky/Monticello</td>
<td>Knox_IN</td>
<td>La_Paz</td>
</tr>
<tr>
<td>Lima</td>
<td>Los_Angeles</td>
<td>Louisville</td>
<td>Maceio</td>
<td>Managua</td>
</tr>
<tr>
<td>Manaus</td>
<td>Martinique</td>
<td>Mazatlan</td>
<td>Mendoza</td>
<td>Menominee</td>
</tr>
<tr>
<td>Merida</td>
<td>Mexico_City</td>
<td>Miquelon</td>
<td>Monterrey</td>
<td>Montevideo</td>
</tr>
<tr>
<td>Montreal</td>
<td>Montserrat</td>
<td>Nassau</td>
<td>New_York</td>
<td>Nipigon</td>
</tr>
<tr>
<td>Nome</td>
<td>Noronha</td>
<td>North_Dakota/Center</td>
<td>Panama</td>
<td>Pangnirtung</td>
</tr>
<tr>
<td>Paramaribo</td>
<td>Phoenix</td>
<td>Port-au-Prince</td>
<td>Porto_Acre</td>
<td>Port_of_Spain</td>
</tr>
<tr>
<td>Porto_Velho</td>
<td>Puerto_Rico</td>
<td>Rainy_River</td>
<td>Rankin_Inlet</td>
<td>Recife</td>
</tr>
<tr>
<td>Regina</td>
<td>Rio_Branco</td>
<td>Rosario</td>
<td>Santiago</td>
<td>Santo_Domingo</td>
</tr>
<tr>
<td>Sao_Paulo</td>
<td>Scoresbysund</td>
<td>Shiprock</td>
<td>St_Johns</td>
<td>St_Kitts</td>
</tr>
<tr>
<td>St_Lucia</td>
<td>St_Thomas</td>
<td>St_Vincent</td>
<td>Swift_Current</td>
<td>Tegucigalpa</td>
</tr>
<tr>
<td>Thule</td>
<td>Thunder_Bay</td>
<td>Tijuana</td>
<td>Tortola</td>
<td>Vancouver</td>
</tr>
<tr>
<td>Virgin</td>
<td>Whitehorse</td>
<td>Winnipeg</td>
<td>Yakutat</td>
<td>Yellowknife</td>
</tr>
</tbody>
</table>

### Antarctica

<table>
<thead>
<tr>
<th>Casey</th>
<th>Davis</th>
<th>DumontDuRville</th>
<th>Mawson</th>
<th>McMurdо</th>
</tr>
</thead>
<tbody>
<tr>
<td>Palmer</td>
<td>South_Pole</td>
<td>Syowa</td>
<td>Vostok</td>
<td>Arctic/Longyearbyen</td>
</tr>
</tbody>
</table>

### Asia

<table>
<thead>
<tr>
<th>Aden</th>
<th>Almaty</th>
<th>Amman</th>
<th>Anadyr</th>
<th>Aqtau</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aqtobe</td>
<td>Ashgabat</td>
<td>Ashkhabad</td>
<td>Baghdad</td>
<td>Bahrain</td>
</tr>
<tr>
<td>Baku</td>
<td>Bangkok</td>
<td>Beijing</td>
<td>Beirut</td>
<td>Bishkek</td>
</tr>
<tr>
<td>Brunei</td>
<td>Calcutta</td>
<td>Choibalsan</td>
<td>Chongqing</td>
<td>Chungking</td>
</tr>
<tr>
<td>Colombo</td>
<td>Dacca</td>
<td>Damascus</td>
<td>Dhaka</td>
<td>Dili</td>
</tr>
<tr>
<td>Dubai</td>
<td>Dushanbe</td>
<td>Gaza</td>
<td>Harbin</td>
<td>Hong_Kong</td>
</tr>
<tr>
<td>Hovd</td>
<td>Irkutsk</td>
<td>Istanbul</td>
<td>Jakarta</td>
<td>Jayapura</td>
</tr>
<tr>
<td>Jerusalem</td>
<td>Kabul</td>
<td>Kamchatka</td>
<td>Karachi</td>
<td>Kashgar</td>
</tr>
<tr>
<td>Katmandu</td>
<td>Krasnoyarsk</td>
<td>Kuala_Lumpur</td>
<td>Kuching</td>
<td>Kuwait</td>
</tr>
<tr>
<td>Macao</td>
<td>Macau</td>
<td>Magadan</td>
<td>Makassar</td>
<td>Manila</td>
</tr>
<tr>
<td>Muscat</td>
<td>Nicosia</td>
<td>Novosibirsk</td>
<td>Omsk</td>
<td>Oral</td>
</tr>
<tr>
<td>Phnom_Penh</td>
<td>Pontianak</td>
<td>Pyongyang</td>
<td>Qatar</td>
<td>Qyzylorda</td>
</tr>
<tr>
<td>Rangoon</td>
<td>Riyadh</td>
<td>Riyadh87</td>
<td>Riyadh88</td>
<td>Riyadh89</td>
</tr>
<tr>
<td>City</td>
<td>City</td>
<td>City</td>
<td>City</td>
<td>City</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------</td>
<td>---------------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Saigon</td>
<td>Sakhalin</td>
<td>Samarkand</td>
<td>Seoul</td>
<td>Shanghai</td>
</tr>
<tr>
<td>Singapore</td>
<td>Taipei</td>
<td>Tashkent</td>
<td>Tbilisi</td>
<td>Tehran</td>
</tr>
<tr>
<td>Tel_Aviv</td>
<td>Thimbu</td>
<td>Thimphu</td>
<td>Tokyo</td>
<td>Ujung_Pandang</td>
</tr>
<tr>
<td>Ulaanbaatar</td>
<td>Ulan_Bator</td>
<td>Urumqi</td>
<td>Vientiane</td>
<td>Vladivostok</td>
</tr>
<tr>
<td>Yakutsk</td>
<td>Yekaterinburg</td>
<td>Yerevan</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Atlantic**

<table>
<thead>
<tr>
<th>City</th>
<th>City</th>
<th>City</th>
<th>City</th>
<th>City</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azores</td>
<td>Bermuda</td>
<td>Canary</td>
<td>Cape_Verde</td>
<td>Faeroe</td>
</tr>
<tr>
<td>Jan_Mayen</td>
<td>Madeira</td>
<td>Reykjavik</td>
<td>South_Georgia</td>
<td>St_Helena</td>
</tr>
<tr>
<td>Stanley</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Australia**

<table>
<thead>
<tr>
<th>City</th>
<th>City</th>
<th>City</th>
<th>City</th>
<th>City</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACT</td>
<td>Adelaide</td>
<td>Brisbane</td>
<td>Broken_Hill</td>
<td>Canberra</td>
</tr>
<tr>
<td>Darwin</td>
<td>Hobart</td>
<td>LHI</td>
<td>Lindeman</td>
<td>Lord Howe</td>
</tr>
<tr>
<td>Melbourne</td>
<td>NSW</td>
<td>North</td>
<td>Perth</td>
<td>Queensland</td>
</tr>
<tr>
<td>South</td>
<td>Sydney</td>
<td>Tasmania</td>
<td>Victoria</td>
<td>West</td>
</tr>
<tr>
<td>Yancowinna</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Brazil**

<table>
<thead>
<tr>
<th>City</th>
<th>City</th>
<th>City</th>
<th>City</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acre</td>
<td>DeNoronha</td>
<td>East</td>
<td>West</td>
</tr>
</tbody>
</table>

**Canada**

<table>
<thead>
<tr>
<th>City</th>
<th>City</th>
<th>City</th>
<th>City</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atlantic</td>
<td>Central</td>
<td>East-Saskatchewan</td>
<td>Eastern</td>
</tr>
<tr>
<td>Mountain</td>
<td>Newfoundland</td>
<td>Pacific</td>
<td>Saskatchewan</td>
</tr>
<tr>
<td>Yukon</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Chile**

<table>
<thead>
<tr>
<th>City</th>
<th>City</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Continental</td>
</tr>
<tr>
<td></td>
<td>EasterIsland</td>
</tr>
</tbody>
</table>

**Etc**

<table>
<thead>
<tr>
<th>Time Zone</th>
<th>Time Zone</th>
<th>Time Zone</th>
<th>Time Zone</th>
<th>Time Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMT</td>
<td>GMT+0</td>
<td>GMT+1</td>
<td>GMT+2</td>
<td>GMT+3</td>
</tr>
<tr>
<td>GMT+4</td>
<td>GMT+5</td>
<td>GMT+6</td>
<td>GMT+7</td>
<td>GMT+8</td>
</tr>
<tr>
<td>GMT+9</td>
<td>GMT+10</td>
<td>GMT+11</td>
<td>GMT+12</td>
<td>GMT0</td>
</tr>
<tr>
<td>GMT-0</td>
<td>GMT-1</td>
<td>GMT-2</td>
<td>GMT-3</td>
<td>GMT-4</td>
</tr>
<tr>
<td>GMT-5</td>
<td>GMT-6</td>
<td>GMT-7</td>
<td>GMT-8</td>
<td>GMT-9</td>
</tr>
<tr>
<td>GMT-10</td>
<td>GMT-11</td>
<td>GMT-12</td>
<td>GMT-13</td>
<td>GMT-14</td>
</tr>
</tbody>
</table>
## Europe

<table>
<thead>
<tr>
<th>Time Zone</th>
<th>City</th>
<th>Time Zone</th>
<th>City</th>
<th>Time Zone</th>
<th>City</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greenwich</td>
<td></td>
<td>UCT</td>
<td></td>
<td>Universal</td>
<td></td>
</tr>
<tr>
<td>Greenwich</td>
<td></td>
<td>UTC</td>
<td></td>
<td></td>
<td>Zulu</td>
</tr>
</tbody>
</table>

### GMT

<table>
<thead>
<tr>
<th>Time Zone</th>
<th>Time Zone</th>
<th>Time Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMT</td>
<td>GMT+1</td>
<td>GMT+2</td>
</tr>
<tr>
<td>GMT+5</td>
<td>GMT+6</td>
<td>GMT+7</td>
</tr>
<tr>
<td>GMT+10</td>
<td>GMT+11</td>
<td>GMT+12</td>
</tr>
<tr>
<td>GMT-2</td>
<td>GMT-3</td>
<td>GMT-4</td>
</tr>
<tr>
<td>GMT-7</td>
<td>GMT-8</td>
<td>GMT-9</td>
</tr>
<tr>
<td>GMT-12</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Indian (Indian Ocean)

<table>
<thead>
<tr>
<th>Time Zone</th>
<th>City</th>
<th>Time Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antananarivo</td>
<td>Chagos</td>
<td>Christmas</td>
</tr>
<tr>
<td>Kerguelen</td>
<td>Mahe</td>
<td>Maldives</td>
</tr>
<tr>
<td>Reunion</td>
<td></td>
<td>Mauritius</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mayotte</td>
</tr>
</tbody>
</table>

### Mexico

<table>
<thead>
<tr>
<th>Time Zone</th>
<th>City</th>
</tr>
</thead>
<tbody>
<tr>
<td>BajaNorte</td>
<td>BajaSur</td>
</tr>
<tr>
<td></td>
<td>General</td>
</tr>
</tbody>
</table>

### Miscellaneous

<table>
<thead>
<tr>
<th>Time Zone</th>
<th>City</th>
<th>Time Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arctic/Longyearbyen</td>
<td>CET</td>
<td>CST6CDT</td>
</tr>
<tr>
<td>Egypt</td>
<td>Eire</td>
<td>EST</td>
</tr>
<tr>
<td>GB</td>
<td>GB-Eire</td>
<td>Greenwich</td>
</tr>
</tbody>
</table>

---

**Time Zones**
<table>
<thead>
<tr>
<th>Country</th>
<th>Zone</th>
<th>Zone</th>
<th>Zone</th>
<th>Zone</th>
<th>Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iceland</td>
<td>Iran</td>
<td>Israel</td>
<td>Jamaica</td>
<td>Japan</td>
<td></td>
</tr>
<tr>
<td>Kwajalein</td>
<td>Libya</td>
<td>MET</td>
<td>MST</td>
<td>MST7MDT</td>
<td></td>
</tr>
<tr>
<td>Navajo</td>
<td>NZ</td>
<td>NZ-CHAT</td>
<td>Poland</td>
<td>Portugal</td>
<td></td>
</tr>
<tr>
<td>PRC</td>
<td>PST8PDT</td>
<td>ROC</td>
<td>ROK</td>
<td>Singapore</td>
<td></td>
</tr>
<tr>
<td>Turkey</td>
<td>UCT</td>
<td>Universal</td>
<td>UTC</td>
<td>WET</td>
<td></td>
</tr>
<tr>
<td>W-SU</td>
<td>Zulu</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Pacific**

<table>
<thead>
<tr>
<th>Location</th>
<th>Zone</th>
<th>Zone</th>
<th>Zone</th>
<th>Zone</th>
<th>Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apia</td>
<td>Auckland</td>
<td>Chatham</td>
<td>Easter</td>
<td>Efate</td>
<td></td>
</tr>
<tr>
<td>Enderbury</td>
<td>Fakaofo</td>
<td>Fiji</td>
<td>Funafuti</td>
<td>Galapagos</td>
<td></td>
</tr>
<tr>
<td>Gambier</td>
<td>Guadalcanal</td>
<td>Guam</td>
<td>Honolulu</td>
<td>Johnston</td>
<td></td>
</tr>
<tr>
<td>Kirritimati</td>
<td>Kosrae</td>
<td>Kwajalein</td>
<td>Majuro</td>
<td>Marquesas</td>
<td></td>
</tr>
<tr>
<td>Midway</td>
<td>Nauru</td>
<td>Niue</td>
<td>Norfolk</td>
<td>Noumea</td>
<td></td>
</tr>
<tr>
<td>Pago_Pago</td>
<td>Palau</td>
<td>Pitcairn</td>
<td>Ponape</td>
<td>Port_Moresby</td>
<td></td>
</tr>
<tr>
<td>Rarotonga</td>
<td>Saipan</td>
<td>Samoa</td>
<td>Tahiti</td>
<td>Tarawa</td>
<td></td>
</tr>
<tr>
<td>Tongatapu</td>
<td>Truk</td>
<td>Wake</td>
<td>Wallis</td>
<td>Yap</td>
<td></td>
</tr>
</tbody>
</table>

**System V**

<table>
<thead>
<tr>
<th>Zone</th>
<th>Zone</th>
<th>Zone</th>
<th>Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>AST4</td>
<td>AST4ADT</td>
<td>CST6</td>
<td>CST6CDT</td>
</tr>
<tr>
<td>EST5EDT</td>
<td>HST10</td>
<td>MST7</td>
<td>MST7MDT</td>
</tr>
<tr>
<td>PST8PDT</td>
<td>YST9</td>
<td>YST9YDT</td>
<td></td>
</tr>
</tbody>
</table>

**US (United States)**

<table>
<thead>
<tr>
<th>Zone</th>
<th>Zone</th>
<th>Zone</th>
<th>Zone</th>
<th>Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alaska</td>
<td>Aleutian</td>
<td>Arizona</td>
<td>Central</td>
<td>East-Indiana</td>
</tr>
<tr>
<td>Eastern</td>
<td>Hawaii</td>
<td>Indiana-Starke</td>
<td>Michigan</td>
<td>Mountain</td>
</tr>
<tr>
<td>Pacific</td>
<td>Samoa</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Aliases**

GMT=Greenwich, UCT, UTC, Universal, Zulu CET=MET (Middle European Time)
Eastern=Jamaica Mountain=Navajo
This appendix provides an overview of the security configuration settings available for the Data Domain system, including secure deployment and usage settings, and the secure maintenance and physical security controls that ensure secure operation.

The following topics are covered:

- Data Domain System Security Overview ................................................................. 52
- Security Configuration Settings ............................................................................. 52
- Secure Maintenance: Data Migration ..................................................................... 66
- Physical Security Controls ..................................................................................... 67
Data Domain System Security Overview

The Data Domain system is an appliance that runs the DD OS embedded operating system. Additional software or agents cannot be installed or executed within a Data Domain appliance. This restriction ensures control and consistency of DD OS releases and provides additional security.

Data Domain systems are viewed as a purpose-built appliance with restricted access to their internal operation; any tampering voids the warranty. EMC incorporates new releases of embedded open-source modules into DD OS versions as appropriate.

Hosts and backup applications interface with the Data Domain systems through one or more of the standard native server interface protocols: CIFS/NFS, NDMP, VTL, or EMC Data Domain Boost. You can mount a network share on the Data Domain directly (server direct) via one of the standard network file sharing protocols: CIFS or NFS.

Access control and user authentication to the Data Domain system is controlled either by local users, NIS environments, or within a Microsoft Active Directory Domain environment.

The following Data Domain native protocols and software options depend on or enable security attributes of the Data Domain system. See the EMC Data Domain Operating System Administration Guide for more information.

- **Supported Native Ingest protocols.** Data Domain systems support simultaneous access via common network access protocols, allowing both backup servers and application servers to send data to the Data Domain system. Servers can attach and transfer files and backup images over one or more of these protocols: CIFS, NFS, EMC Data Domain Boost, NDMP, and VTL over fibre channel. Because data moved over these protocols are transported “in the clear” and no encryption is supported for data transfers over these protocols, user authentication and access control to the related network ports is of critical importance.

- **EMC Data Domain Replicator software** provides automated, policy-based, network-efficient replication for disaster recovery, remote office data protection, and multi-site tape consolidation. DD Replicator software asynchronously replicates only the compressed, deduplicated data over the WAN during the backup process, making network-based replication fast, reliable, and cost-effective. For environments that do not leverage a VPN for secure connections between sites, DD Replicator software can securely encapsulate its replication payload over SSL with AES 256 bit encryption for secure transmission over the wire.

- **EMC Data Domain Encryption software** is an administratively enabled option set using the CLI or Data Domain System Manager. It protects backup and archive data stored on Data Domain systems with data encryption that is performed inline before the data is written to disk. Encrypting data at rest satisfies internal governance rules and compliance regulations and protects against the reading of customer data on individual disks or disk shelves removed from the system due to theft.

- **DD Retention Lock** prevents specified files from being overwritten, modified, or deleted for a user-defined retention period of up to 70 years, or until January 19, 2038, if you are using NFS, because of protocol constraints.

Security Configuration Settings

The following security setting categories are discussed:

- Access control settings, which are under administrative control, limit access by end users and external product components.

- Log settings relate to the logging of events.
Communication security settings relate to security for the product network communications.

Data security settings ensure protection of the data associated with the product.

Secure serviceability settings are available to ensure control of service operations performed on the products by EMC or its service partners.

Security alert system settings relate to sending security alerts and notifications for security-related events.

Additional security considerations: EMC Data Domain Retention Lock, dual sign-on requirements, and the secure system clock.

### Access Control Settings

The Data Domain operating environment provides secure administrativestratation by one of the following methods. Either method allows locally defined users, Network Information Service (NIS) users, and Microsoft Active directory domain users.

- Data Domain System Manager via HTTPS. The Data Domain system can use its self-signed identity certificate to establish a trusted connection to manage the Data Domain system over SSL.

- SSH for CLI. The administrator enters a controlled shell environment, where individual CLI commands are executed to manage the Data Domain system.

Administrative system access can be either Local or Remote.

- **Local Access**
  CLI via serial or over the IP local access is available for authorized administrators who are on the same subnet and have proper login credentials (username and password). For access, the user is prompted for the username and password; once validated the user enters the default controlled user CLI shell environment.

  **Note**

  Policies should be put in place for users to log out after the session is over. No other access method (such as remote dial-in or a physical RS-232 connection) to the appliance is available.

- **Remote Access**
  CLI and Web-based System Manager remote access are available for authorized administrators with proper login credentials (username and password). Remote users with network access and authorization can remotely administer the Data Domain systems over the network.

  **Note**

  By default only secure shell (SSH) and secure browsing (HTTPS) is enabled on the Data Domain system. SSH also supports password-less login.

  EMC recommends configuring session timeout values in Data Domain System Manager to ensure users are automatically logged out of the system after the session is over. The timeout needs to be longer than the maximum configuration time. For example, the worst case for DHCP configuration is 90 seconds. Session timeout should be no less than five minutes.

Data Domain systems feature security protocols to control access to the data residing on the system. Data is not readily viewable from anywhere except a host that has been granted access. The following main access control methods are available in a Data Domain system:
Host-based access lists
Administrator access is required to configure the Data Domain appliance and adjust which physical hosts can view an exported mount point. Those with administrative access can update the access list with a server's hostname or IP address. A Data Domain system can use DNS for name resolution; for greater protection, administrators can hard code entries in the hosts file to control hosts/port resolution.

File Permissions
Files created on the Data Domain system are “owned” by the creator. For example, backup software typically writes files as a particular user, so that user would own all files that the backup software created on the system. Explicit Windows permissions (ACLs) must be set, however, to prevent users from viewing files created by others.

Microsoft CIFS
For every file or folder created through CIFS, the following attributes are created:
- Owner SID
- Group SID
- DACL (Discretionary ACL – Permissions)
- SACL (System ACL – Auditing Information)
- DOS Attributes such as READONLY, HIDDEN, SYSTEM & ARCHIVE
In addition, folders and files map Unix UID/GID/MODE from Windows Owner-SID/Group-SID/DACL. The DACL is inherited from its parent. If the parent directory does not have DACL (created though NFS/non-CIFS), then a default ACL is assigned. The default gives the owner full control and gives others read permission. Access control is managed through the standard Microsoft MMC on any client with permissions to do so.

Linux NFS
Files and folders created through the remaining ingest protocols use the POSIX.1e ACL standard. Every object is associated with three sets of permissions that define access for the owner, the owning group, and for others. Each set may contain Read (r), Write (w), and Execute (x) permissions. This scheme is implemented using only nine bits for each object. In addition to these nine bits, the Set User Id, Set Group Id, and Sticky bits are used for a number of special cases. Access control is managed through a standard Linux client or Data Domain system CLI administration environment with permissions to do so.

Microsoft Active Directory Services
Data Domain systems can utilize Microsoft Active Directory pass-through authentication for the users/servers. Admins can enable certain domains and groups of users to access files stored on the Data Domain system.

NIS Directory Services
Data Domain systems can utilize NIS Directory Authentication for the users in UNIX/LINUX environments. Administrators can enable specific hosts and users to access files stored on the Data Domain system.

The combination of a host-based access list along with local users or domain directory services allows the administrator to control which users and servers have permissions to view data on a Data Domain system.

Separate NFS and CIFS shares
Admins can easily create shares on the Data Domain file system. Using the native access control methods helps to define more granular share/directory/file-level access control over certain data on the Data Domain system. For example, when setting up a shared system for multiple customers, administrators can have a NFS or CIFS share created for each specific customer on the same Data Domain system and specify access controls for each customer/share.
The following access control settings are described:

- Default Accounts
- Authentication Configuration
- User Authorization
- Component Access Control
- Component Authentication
- Component Authorization

Default Accounts

- `sysadmin` is the default user account on the DD system. During the initial configuration the administrator who logs in as sysadmin is prompted to change the password. The sysadmin account cannot be deleted.
- The default password is the Data Domain system’s serial number or service tag number.

Authentication Configuration

For instructions on changing default account passwords and deleting accounts that are no longer in use, see Managing Data Domain Systems in the EMC Data Domain Operating System Administration Guide.

Data Domain System Integration into Microsoft's Active Directory (AD)

With the latest version of the DD OS installed, follow this procedure.

Procedure

1. Determine authentication mode and verify connectivity.
   a. Determine the authentication mode configuration on the Data Domain system by entering: `# cifs show config`  
      If the mode is Workgroup or Domain, the system is not configured for AD.
      If the mode is Active-Directory, the system is using Active Directory Authentication (Windows 2000 and later). Whether or not the system is properly communicating with AD, however, is not verified.
   b. To verify connectivity to AD, look up a non-administrator AD user using the CIFS troubleshooting command. Enter: `# cifs troubleshooting user user name`  
      If the user cannot be found, the Data Domain system is not communicating with AD.
      If details of the AD user are listed, such as user and group and their IDs, the Data Domain system is successfully communicating with AD.

2. Prepare the Data Domain system to join AD if the system is not configured or not communicating with AD.
   a. If the authentication mode is currently set to Domain or Active Directory Mode, configure the Data Domain system for Workgroup Mode by entering:
      `# cifs set authentication workgroup workgroup`
   b. Verify DNS settings on the Data Domain system. Enter:
      `# net show dns`  
   c. To change the DNS server, enter:
      `# net set dns dns server ip`
d. Test IP connectivity from the Data Domain system to the DNS server.
   
   ```
   # net ping dns server ip count 3
   ```

e. Confirm the AD domain. Access a DOS prompt on a Windows computer (server or
   client does not matter). At the Windows DOS prompt, enter:

   ```
   set
   USERDNSDOMAIN= is the domain name that is used when setting the domain
   name on the Data Domain system.
   ```

   f. Confirm the Data Domain system domain name by entering:

   ```
   # net show domainname
   ```
   If the domain name is not correct, enter:

   ```
   # net set domainname domain name
   ```

   g. Confirm that the domain name responds to the command net ping.

   ```
   # net ping domain name count 3
   ```
   If net ping does not respond, make sure the correct DNS server has been
   specified.

   h. Confirm the Data Domain system’s host name.

   ```
   # net show hostname
   ```
   If the host name is not correct, set it to the correct name:

   ```
   # net set hostname host name
   ```

3. (Optional) If you have a server that is running the Network Time Service (NTP) you can
   choose to configure NTP at this time. See the EMC Data Domain Operating System
   Administration Guide.

4. Verify the Data Domain system’s system clock and compare the time with the AD
   domain controller. Enter:

   ```
   # date
   ```
   To modify the time, enter:

   ```
   # system set date MMDDhhmm[[CC]Y]
   ```
   Compare the Data Domain system’s system clock with the AD domain controller. They
   must be within 5 minutes of each other.

5. Join the Data Domain system to AD.

   To successfully join the Data Domain system to AD, the Windows administrator
   account must have the correct permissions.

   Verify that administrator account password does not contain spaces, right and left
   square brackets ([,]), or the dollar sign ($).

   Enter:

   ```
   # cifs set authentication active-directoryrealm domain controller ip address, *
   ```
   For example:

   ```
   # cifs set authentication active-directory olympus.local 123.456.78.90, *
   ```

6. To verify connectivity to AD, look up a (non-administrator) AD, enter:

   ```
   # cifs troubleshooting user user name
   ```
   If the details of the AD user are listed, the Data Domain system is successfully
   communicating with AD.
7. To verify that the Data Domain system host is listed in AD, check that the Data Domain system host is listed in the computer container in the Active Directory (Active Directory Users and Computers page).

8. Ensure backups are working. Run a backup to the Data Domain system and verify that it finishes without errors.

Actions Not Requiring Authentication

Most, but not all show commands and viewing of statistics do not require authentication.

User Authorization

User authorization settings control rights or permissions that are granted to a user to access a resource managed by the Data Domain system.

A Data Domain system supports five classes of users:

- **User.** This is the class for standard users who have access to a limited number of operations and commands. The user class can view configuration information only.

- **Admin.** This is the class for administrators who have access to all Data Domain system operations and commands. Administrators cannot view the actual user data stored on the Data Domain system directly, but can copy the data off the unit to an external client location.

- **Sysadmin.** This is the default user account on a Data Domain system. During the initial configuration the sysadmin is prompted to change the password. This account cannot be deleted, but the password can be changed after the administrator has logged in.

- **Security Officer.** This is the class for enabling/disabling a specific set of security functions. In DD OS 5.0 or later, the security officer class is one of the two users required for DD Encryption lock/unlock, and for changing the encryption passphrase. Security officer is also required for Retention Lock compliance.

- **Backup Operator.** This class, which is available with DD OS 5.2 or later, has a predefined set of controls to manage specific backup and recovery related tasks that include:
  - Add and delete SSH public keys for password-less log-in (mostly used for automated scripting)
  - Add, delete, reset and view CLI command aliases
  - View configuration and settings related to alerts, autosupport, NIS, CIFS, DD Boost, storage, file system, cleaning, network, MTrees, NFS, NTP, Replication, Route, SNMP, snapshot, system, users, logs, and so forth.
  - Perform a fast copy of data from a source to destination path
  - Perform the syncing of all modified files
  - Wait for replication to complete on the destination system
  - Create snapshots for MTrees
  - Change password for a user
  - Import/export and move tapes between elements in a Virtual Tape Library
  - View all VTL configuration.

System Passwords

Password management is an integral part of DD OS. Managed by the admin user, a password can be set for individual users with a variety of controls:
Minimum Days Between Change: The minimum number of days between password changes that you allow a user. The default is 0.

Maximum Days Between Change: The maximum number of days between password changes that you allow a user. The default is 99999.

Warn Days Before Expire: The number of days to warn the users before their password expires. The default is 7.

Disable Days After Expire: The number of days after a password expires to disable the user account. The default is Never.

Disable Account on the Following Date: The option to select an account and enter a date (mm/dd/yyyy) when you want to disable it. The default is no date.

For uniform password management across the enterprise, a default password policy can be changed and applied to all newly created passwords with the default policy set.

Local Users
The local users reside on the Data Domain system, and are either created through CLI or through DD System Manager. UIDs are assigned in the range of 500-10,000 to local users. When an access request comes in through one of the network interfaces, the DD OS does a look-up on the user first to determine if it already has the user in its local user list.

New local users can be added or deleted, by the Data Domain administrator, for login access to a Data Domain system. The new user can either be a regular user with limited functionality or an admin user to perform administrative tasks. Backup Operator and Security Officer users, are also local users.

Note
All user account information is stored in the root file system and not accessible via controlled CLI or GUI.

Domain Users
If the Data Domain system does not find the user in its local file, it will make an external request on the network to the configured Domain Directory Services Server to resolve and acknowledge the requesting user’s access rights and permissions. This is known as pass-through authentication. The Data Domain Operating System supports two types of external domain pass-through authentication:

Microsoft Active Directory Services: A protocol for managing users, host names, and access rights among systems on a network, primarily for Microsoft environments.

NIS (Network Information Service): A rudimentary, but functional directory service protocol for distributing system configuration data supporting users on a network, primarily for UNIX/LINUX environments.

Component Authentication
For instructions about how to configure authentication of remote components, see Managing Network Connections in the EMC DD OS Administration Guide.

Component Authorization
For instructions about how to configure the product to restrict access to remote components or systems, such as IP filtering, see Managing Network Connections in the EMC Data Domain Operating System Administration Guide.

Log Settings
A log is a chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities
surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results.

All Data Domain system logs (system, space, errors, access related) are stored on the root file system partition, and not accessible directly except through these services:

- Logs can be sent to a remote syslog server for long-term archiving via FTP or SCP (authorized support personnel only).
- Logs can be accessed via successful login via the CLI or the System Manager.

The Data Domain system log file entries contain messages from the alerts feature, autosupport reports, and general system messages. The log directory is /ddvar/log.

For more information, see Managing Log Files in the *EMC Data Domain Operating System Administration Guide*.

**Communication Security Settings**

Communication security settings enable the establishment of secure communication channels between the product components as well as between product components and external systems or components.

**Port Usage**

The System Manager uses HTTP port 80 and HTTPS port 443. If your Data Domain system is behind a firewall, to reach the systems, you might need to enable port 80 if using HTTP, or port 443 if using HTTPS. The port numbers can be easily changed if security requirements dictate.

Traps are sent out through port 162.

When adding a DD System to the Data Domain System Manager: If a port is configured, enter a Custom Port instead of the default port 3009.

**Administration/Support Protocols**

The Data Domain system supports several services and protocols for administration. Telnet is used to access the controller. The CLI environment is disabled by default. You can enable it from the Web-based Data Domain System Manager's System Settings > Access Management page (Port 23).

These services and protocols include:

- **HTTP/HTTPS** is used to access the Data Domain System Manager. Open either Port 80 or secure Port 443. HTTPS uses the Data Domain system’s internally generated signed certificate to establish a trust between the client and the Data Domain system’s Web browser. SSH is used to access the Data Domain CLI (Port 22). You can enable it from the Data Domain System Manager via the System Settings > Access Management page.

- FTP, FTPS and SCP are used to download logs, autosupport files and support bundles, and can be used to upload DD OS Upgrade RPM files.

  FTP is an insecure protocol that allows passwords to pass unencrypted over the network.

  FTPS or SCP are recommended as secure file transfer methods of administrative files.

- **Secure Copy (SCP)** is used by Support to securely copy or move internal system files such as system logs in and out of the Data Domain system. SCP is available to any admin user and uses the same port as SSH (Port 22). It is enabled by default.
- FTP is used for moving files to and from the Data Domain system for maintenance purposes only (Port 20/21). It can be enabled via the System Settings > Access Management page.

Note

As of DD OS 5.3, SFTP is supported.

- Secure Copy (SCP) is used by Support to securely copy or move internal system files such as system logs in and out of the Data Domain system. SCP is available to any admin user and uses the same port as SSH (Port 22). It is enabled by default.

Data Transfer Protocols

Protocols that can be enabled on a Data Domain system to ingest data from a server and to restore data to a server include:

- NFS (v3 over TCP only) – UNIX/LINUX file sharing protocol
- CIFS (SMB 1 only) - Microsoft network file sharing protocol
- EMC Data Domain Boost – A client-side plug-in with a proprietary protocol over IP networks. As of DD OS 5.3, EMC DD Boost is also available over Fibre Channel networks. It is designed to optimize and accelerate backup software and product application interaction with Data Domain systems. By distributing parts of the deduplication process to the backup server or application client, EMC DD Boost speeds up aggregate backup throughput on Data Domain systems up to 50 percent, while reducing load on LANs.
- Data Domain Virtual Tape Library –Tape emulation over Fibre Channel
- NDMP - an open protocol for transporting data between NAS devices and a Data Domain system

Other protocols that can be enabled on a Data Domain system include:

- SNMP – An industry standard protocol for sending and monitoring MIB data.
- SSL – An industry standard protocol used to encapsulate the payload while data is in flight for secure replication between Data Domain systems.

Data Domain TCP and UDP Ports

**Table 3 Data Domain System Inbound Communication Ports**

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 21</td>
<td>FTP</td>
<td>Port is used only if FTP is enabled. Run <code>adminaccess show</code> on the Data Domain system to determine if it is enabled.</td>
</tr>
<tr>
<td>TCP 22</td>
<td>SSH &amp; SCP</td>
<td>Port is used only if SSH is enabled. Run <code>adminaccess show</code> on the Data Domain system to determine if it is enabled. SCP is enabled as default</td>
</tr>
<tr>
<td>TCP 23</td>
<td>Telnet</td>
<td>Port is used only if Telnet is enabled. Run <code>adminaccess show</code> on the Data Domain system to determine if it is enabled.</td>
</tr>
</tbody>
</table>
### Table 3 Data Domain System Inbound Communication Ports (continued)

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 80</td>
<td>HTTP</td>
<td>Port is used only if HTTP is enabled. Run <code>adminaccess show</code> on the Data Domain system to determine if it is enabled.</td>
</tr>
<tr>
<td>TCP 111</td>
<td>EMC DD Boost / NFS (portmapper)</td>
<td>Used to assign a random port for the mountd service used by EMC DD Boost and NFS. Mountd service port can be statically assigned.</td>
</tr>
<tr>
<td>TCP 123</td>
<td>NTP</td>
<td>Port is used only if NTP is enabled on the Data Domain system. Run <code>ntpq status</code> to determine if it is enabled.</td>
</tr>
<tr>
<td>UDP 137</td>
<td>CIFS (NetBIOS Name Service)</td>
<td>Port used by CIFS for NetBIOS name resolution.</td>
</tr>
<tr>
<td>UDP 138</td>
<td>CIFS (NetBIOS Datagram Service)</td>
<td>Port used by CIFS for NetBIOS Datagram Service.</td>
</tr>
<tr>
<td>TCP 139</td>
<td>CIFS (NetBIOS Session Service)</td>
<td>Port used by CIFS for session information.</td>
</tr>
<tr>
<td>TCP 161</td>
<td>SNMP</td>
<td>Port is used only if SNMP is enabled. Run <code>snmp status</code> to determine if it is enabled.</td>
</tr>
<tr>
<td>TCP 443</td>
<td>HTTPS</td>
<td>Port is used only if HTTPS is enabled. Run <code>adminaccess show</code> on the Data Domain system to determine if it is enabled.</td>
</tr>
<tr>
<td>TCP 445</td>
<td>CIFS (Microsoft-DS)</td>
<td>Main port used by CIFS for data transfer.</td>
</tr>
<tr>
<td>TCP 2049</td>
<td>EMC DD Boost / NFS</td>
<td>Main port used by NFS. Can be modified via the <code>nfs reset server-port</code> command. (This command is SE mode, which means that it can be issued only by a Service Engineer.)</td>
</tr>
<tr>
<td>TCP 2051</td>
<td>Replication</td>
<td>Port is used only if replication is configured on the Data Domain system. Run <code>replication show config</code> to determine if it is configured. This port can be modified via the <code>replication modify</code> command.</td>
</tr>
<tr>
<td>*</td>
<td>NFS (mountd)</td>
<td>Can be hardcoded via command <code>nfs reset mountd-port</code> (This command is SE mode, which means that it can be issued only by a Service Engineer.)</td>
</tr>
<tr>
<td>TCP 3009</td>
<td>DDMC Port</td>
<td>This port is used only if the Data Domain system is being managed by the Data Domain Management Center.</td>
</tr>
</tbody>
</table>

### Table 4 Outbound Communication Traffic Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 25</td>
<td>SMTP</td>
<td>Used by the Data Domain system to send email autosupports and alerts.</td>
</tr>
<tr>
<td>TCP 80</td>
<td>HTTP</td>
<td>Used by Data Domain system for uploading log files to Data Domain Support via the <code>support upload</code> command.</td>
</tr>
</tbody>
</table>
Table 4 Outbound Communication Traffic Ports (continued)

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 123</td>
<td>NTP</td>
<td>Used by the Data Domain system to synchronize to a time server.</td>
</tr>
<tr>
<td>TCP 160</td>
<td>SNMP</td>
<td>Used by the Data Domain system to send SNMP traps to SNMP host. Use <code>snmp show trap-hosts</code> to see destination hosts and <code>snmp status</code> to display service status.</td>
</tr>
<tr>
<td>TCP 514</td>
<td>Syslog</td>
<td>Used by the Data Domain system to send syslog messages, if enabled. Use <code>log host show</code> to display destination hosts and service status.</td>
</tr>
<tr>
<td>TCP 2051</td>
<td>Replication</td>
<td>Used by Data Domain system only if replication is configured. Enter <code>replication show config</code> to determine if it is configured.</td>
</tr>
<tr>
<td>TCP 3009</td>
<td>DDMC Port</td>
<td>This port is used only if the Data Domain system is being managed by the Data Domain Management Center.</td>
</tr>
</tbody>
</table>

Network Encryption

The CA and Host certificates need to be compatible with the RSA DPM Key Manager. You can request these certificates from third-party certificates authorities, or create them using appropriate SSL utility tools. For information about encryption certificates and key managers, see Managing Encryption of Data at Rest in the EMC Data Domain Operating System Administration Guide.

For SSL usage with the Data Domain system, see Manage FTP Access and Monitoring Data Domain System in the EMC Data Domain Operating System Administration Guide.

DD Replicator supports encryption of data-in-flight by using standard Secure Socket Layer (SSL). For information about encrypting replicated data, see Working with Replication in the EMC Data Domain Operating System Administration Guide.

Externally Signed Certificate of Authority (CA)

If the Data Domain system uses the RSA Data Protection Manager external encryption key manager, it requires a PKCS12 host certificate and an external Certificate of Authority in PEM (public certificate) format in order to establish a trusted connection between the RSA Data Protection Manager Server and each Data Domain system that it manages.

The certificate signing requires PKCS10 format. The public certificate key can have either PKCS12 (public plus a private key) or PEM (public) format. The host certificate PEM format is used only with the CSR (Certificate Signing request) feature. Only one external host or CA certificate is allowed for the Data Domain system. HTTPS requires only the host certificate.

If the host certificate has the server/client X509V3v extension, it is used for HTTPS/RSA DPM Key Manager. If the host certificate has no extension, or both client and server extensions, it is used for both RSA DPM Key Manager and HTTPS.

DD OS 5.3 and later support the importation of the host certificate in PKCS12 format. If there is a CSR on the system, you can import the host certificate in PEM format after the CSR is signed by a Certificate Authority.
Note
- The system passphrase is required to import the certificate.
- The system can use only one external host certificate.

Uploading Certificates
You can upload either PEM (public key) or PKCS12 (a public plus a private key) to the Data Domain system via secure FTP in the /ddvar/certificates directory.

Follow these steps:

Procedure
1. From your local machine, copy the host PKCS12 certificate to the Data Domain system by entering:
   
   $ scp Host PKCS12 file admin@Data Domain System: /ddvar/certificates

2. From the Data Domain system, import the host certificate and specify the filename.
   
   # adminaccess certificate import host file Host PKCS12 file

3. When prompted to provide the password to decrypt the PKCS12 file, enter the password.
   
   If the procedure is successful, you are informed that the certificate has been imported.

Self-Signed Certificates
DD OS 5.1 and DD OS 5.2 use the MD5 Message-Digest Algorithm in the self-signed certificate generation process. DD OS 5.3 and later use the SHA1 Message-Digest algorithm for the self-signed certificate.

DDOS 5.3 and later support the generation of CSRs in PKCS10 format. The certificate signing request is available in this location:

/ddvar/certificates/CertificateSigningRequest.csr

You can use either SCP, FTP, or FTPS to obtain the CSR from the Data Domain system.

The command to generate the certificate signing request is:

# adminaccess certificate generate cert-signing-request

Provide the following:
- Private Key strength: The enumeration values allowed are 1024 bit, 2048 bit, or 4096 bit. The default value is 2048 bit.
- Country: The default value is US. This abbreviation cannot exceed two characters. No special characters are allowed.
- State: The default value is California. The maximum entry is 128 characters long.
- City: The default value is Santa Clara. The maximum entry is 128 characters long.
- Organization Name: The default value is My Company Ltd. The maximum entry is 64 characters long.
- Organization Unit: The default value is an empty string. The maximum entry is 64 characters long.
- Common Name: The default value is system hostname. The maximum entry is 64 characters long.
Data Security Settings

Data security settings enable definition of controls to prevent data permanently stored by the product to be disclosed in an unauthorized manner.

Encryption Overview

There are two types of encryption offered with Data Domain systems:

- Encryption of data-at-rest via the Data Domain Encryption software option.
- Encryption of data-in-flight via Data Domain Replicator software, used for replicating data between sites over the WAN.

**DD Encryption: Encryption of Data-at-Rest**

Encryption of data-at-rest protects user data if the Data Domain system is lost or stolen and eliminates accidental exposure if a failed drive needs to be replaced. When the file system is intentionally locked, an intruder who circumvents network security controls and gains access to the Data Domain system will be unable to read the file system without the proper administrative control, passphrase, and cryptographic key. DD Encryption software is completely transparent to the backup or archive application.

DD Encryption provides inline encryption, which means as data is being ingested, the stream is deduplicated, compressed and encrypted using a key before being written to the RAID group. Data Domain Encryption software uses RSA BSAFE libraries, which are FIPS 140-2 validated.

The Data Domain administrator can select a 128-bit or 256-bit Advanced Encryption Standard (AES) algorithm for encrypting all data within the system. One of two cipher modes, Cipher Block Chaining mode (CBC) or Galois/Counter mode (GCM), can be selected to best fit security and performance requirements. In addition, the system leverages a user-defined passphrase to encrypt that key before it is stored in multiple locations on disk. The system encryption key cannot be changed and is not, in any way, accessible to a user. Without the passphrase, the Data Domain file system cannot be unlocked, thus data is not accessible.

With DD OS 4.9/5.0/5.1, when DD Encryption software is enabled, the system randomly generates a single, static system-wide cryptographic strength encryption key.

With DD OS 5.2 or later, an environment that requires encryption keys to be changed on a periodic basis to meet security and compliance regulation can have its encryption key externally managed by RSA DPM. DPM can manage the lifecycle of the encryption key for each Data Domain system. Policies to rotate the encryption key on a periodic basis can be centrally configured using RSA DPM. Keys can also be deleted, expired, or marked as compromised when there is a possibility of a data breach. To further ensure that the encryption keys are safeguarded, a copy of the keys is stored in a second RSA DPM server. In addition, RSA DPM provides audit logs for key state changes that are necessary to prove compliance.

DD OS 5.3 introduces the Data Domain internal Embedded Key Manager. By default, the Data Domain Embedded Key Manager is in effect after you restart the file system unless you configure the RSA DMP Key Manager.

**DD Replicator - Encryption of Data-in-Flight**

Encryption of data-in-flight encrypts data being transferred via DD Replicator software. It uses OpenSSL AES 256-bit encryption to encapsulate the replicated data over the wire. The encryption encapsulation layer is immediately removed as soon as it lands on the destination Data Domain system. Data within the payload can also be encrypted via Data Domain’s encryption software.
Data Erasure

The `filesys destroy` command deletes all data in the Data Domain file system. You can also destroy the file system using the Data Domain System Manager. For more information on commands, see the *EMC Data Domain Operating System Command Reference Guide*. See the *EMC Data Domain Operating System Administration Guide* for information about using the System Manager.

System sanitization was designed to remove all traces of deleted files and restore the system to the state prior to the file’s existence. The primary use of the `sanitize` command is to resolve Classified Message Incidents (CMIs) that occur when classified data is copied inadvertently onto a non-secure system. System sanitization is typically required in government installations.

**Note**

The DD data erasure is not compliant with DoD requirements. For DoD compliance, EMC offers a service Model Number: P5- BAS-DDDE. Information can be found at [http://powerlink.emc.com/km/appmanager/km/secureDesktop?_nfpb=true&_pageLabel=query1&internalId=0b0140668060f2d1&_irrt=true](http://powerlink.emc.com/km/appmanager/km/secureDesktop?_nfpb=true&_pageLabel=query1&internalId=0b0140668060f2d1&_irrt=true)

Secure Serviceability Settings

**Note**

See the section on user roles in the *EMC Data Domain Operating System Administration Guide*. Your contracted support provider has access to settings that are not available to the general administrator.

**EMC Secure Remote Support**

EMC Secure Remote Support (ESRS) is an IP-based automated connect home and remote support solution. ESRS creates both a unified architecture and a common point of access for remote support activities performed on your EMC product. The ESRS IP Solution does the following:

- Provides continuous monitoring, diagnosis, and repair of minor EMC hardware issues.
- Uses the most advanced encryption, authentication, audit, and authorization for ultra-high security remote support.
- Addresses compliance with corporate and governmental regulations by providing logs of all access events.
- Provides easy integration and configuration with your storage management network and firewalls.
- Provides maximum information infrastructure protection. IP-based sessions enable fast information transfer and resolution.
- Consolidates remote support for your EMC information with the ESRS Gateway Client.
- Provides failover protection.
- Provides remote access to your disaster recovery site and makes recovery from unplanned events seamless.
- Protects information in motion or at rest. AES256 encryption during information transfer protects your information.
- Reduces costs and data center clutter and accelerates time to resolution. The elimination of modem/phone line costs translates to lower costs.
EMC Secure Remote Support technical documentation is available on the EMC online support site.

Security Alert System Settings

See the *EMC Data Domain Operating System Administration Guide* for information about how to manage alerts.

**EMC Data Domain Retention Lock Software**

EMC Data Domain Retention Lock software provides immutable file locking and secure data retention capabilities for customers that meet both corporate governance and compliance standards, such as SEC 17a-4(f). DD Retention Lock provides the capability for administrators to apply retention policies at an individual file level. This software enables customers to leverage their existing Data Domain appliances for backup and archive data. DD Retention Lock ensures that archive data is retained long-term with data integrity and secure data retention. DD Retention Lock Governance edition and DD Retention Lock Compliance edition can coexist on the same Data Domain system to enable different retention periods for different classes of archive data. DD Retention Lock software is compatible with industry-standard, NAS-based (CIFS, NFS) Write-Once-Read-Many (WORM) protocols and is qualified with leading archive applications such as EMC SourceOne, EMC DiskXtender, and Symantec Enterprise Vault.

**Dual Sign-On Requirements**

When DD Retention Lock Compliance is enabled on a Data Domain system, additional administrative security is provided in the form of “dual” sign-on. This requires a sign-on by the system administrator as well as a sign-on by a second authorized authority (referred to as “Security Officer”). The “dual” sign-on mechanism of the DD Retention Lock Compliance edition acts as a safeguard against any actions that could potentially compromise the integrity of record files before the expiration of the retention period.

**Secure System Clock**

One of the primary requirements of regulatory compliance standards is time-based retention in which records are preserved exclusively in a non-rewritable, non-erasable format. To meet this requirement a Data Domain system ensures that any undesired changes to the system clock on the Data Domain controller cannot be executed.

**Secure Maintenance: Data Migration**

Data migration offers Data Domain customers the ability to transfer data from one Data Domain system to another for maintenance, which is primarily used for retiring an older system or for upgrading to a newer Data Domain system.

The migration function is available for administrators only and is usually executed over a LAN. Administrators must use the command line interface. The migration command copies all data, metadata, replication contexts (configurations,) and user-configuration information from one Data Domain system to another. Data migration considerations follow:

- Data migration assumes the Data Domain systems are properly configured for the network, with both systems having properly configured security access.
- All data under /backup will be migrated to MTrees that have the same names on both the source and destination systems after the migration.
After migrating replication contexts, the migrated contexts remain on the migration source. The administrator needs to disable replication on the migration source.

Backup operations to the migration source should be paused during migration.

The migration destination does not need a replication license for migration alone.

The migration destination must have a capacity that is the same size as or larger than the used space on the migration source.

The migration destination must have an empty file system.

Migration to a system with Extended Retention software option is supported only if the source system also has the Extended Retention software option.

Physical Security Controls

Physical security controls enable the protection of resources against unauthorized physical access and physical tampering.

The ES20, DD660, and DD690 have a disk-drive locking mechanism that prevents the removal of a disk drive without the appropriate tool, which is a T10 Torx screwdriver. The bezel on the ES30 has a lock and key that prevents access to the drives.

The DD880, DD140, DD160, DD610, DD620, DD630 have no physical access controls. The DD4200, DD4500, DD7200, and the DD990 have E330-style bezels, although there is no key lock on the DD990.

For more information, see the following related EMC documentation for your product: *EMC Data Domain Expansion Shelf Hardware Guide*, the *EMC Data Domain Hardware Guide*, or disk FRU replacement guides.