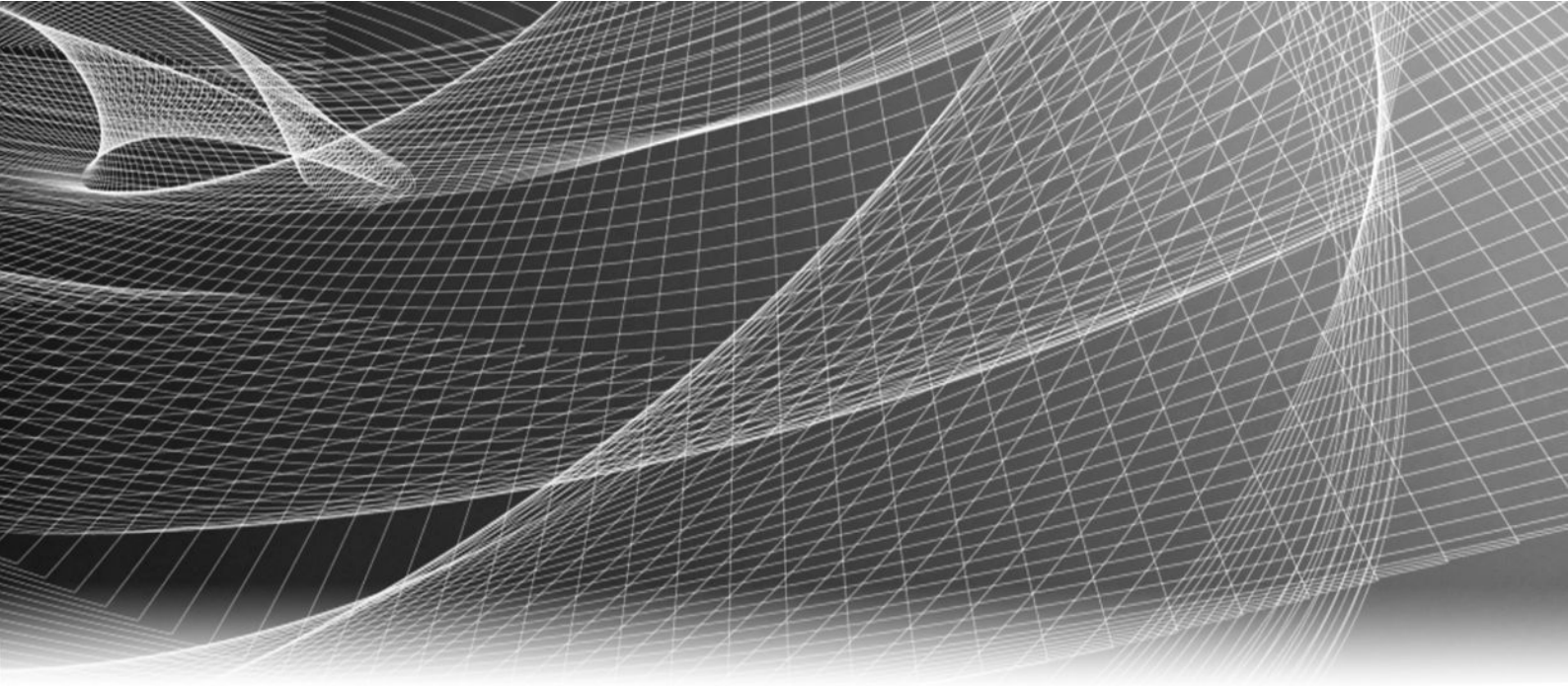


EMC Data Domain Operating System

Version 5.5

Initial Configuration Guide

302-000-478

REV 02

EMC²

Published December, 2014

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.EMC.com

CONTENTS

Preface

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 the EMC Online Support Site to make sure 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 intended for use by 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 particular Data Domain system, provides instructions for installing your Data Domain system, enabling data transfer, powering on the controller, and enabling administrative communication. After you have completed these tasks, this guide provides additional information about configuring your system.

The following Data Domain system documentation provides additional information about the use of your system and can be found on the EMC Online Support Site:

- *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 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*

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:

Table 1 Typography in This Publication

Bold	Indicates interface element names, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what you usually select)
Italic	Highlights publication titles referenced in text
`Monospace`	Indicates system information, such as: • System code • System output, such as an error message or script • Pathnames, filenames, prompts, and syntax • Commands and options
`Monospace italic`	Highlights a variable name that must be replaced with a variable value
`Monospace bold`	Indicates text for user input
[ ]	Indicates optional values
|	Indicates alternate selections - the bar means “or”
{ }	Indicates content that you must specify, such as x or y or z
...	Indicates nonessential information omitted from the example

Contacting Data Domain

To resolve issues with Data Domain products, contact your contracted support provider, or see the EMC Online Support Site.

Your comments

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

Revision History of This Guide

The following table shows the revision history of the *EMC Data Domain Operating System Initial Configuration Guide*.

Table 2 Revision History

Revision	Date	Description
01	May 2014	Initial publication for release 5.5.
02	December 2014	Time Zones appendix updated for release 5.5.1.4

CHAPTER 1

Before Starting Configuration

This chapter describes some steps you must complete before starting your configuration.

Power On the Controller

1. Connect power cables to each receptacle and attach the retention clips. The system immediately powers on when plugged in.
2. Ensure that each power supply is connected to a different power source.

Note

- A new BBU may take up to 3 hours to charge to a sufficient level before the file system is enabled.
- If the battery is good but the system won't boot or if the battery is failing to charge, contact EMC Data Domain Technical Support.

Set Up an Administrative Console

To set up, and log into, an administrative console, follow these steps.

Procedure

1. Connect an administrative console to the serial port at the rear of the system.
2. Log into the Data Domain command-line interface (CLI) as user **`sysadmin`**.

```
# ssh -l sysadmin host-name
```

3. Enter the default password, which is the serial number from the rear panel of your Data Domain system. If you cannot find the serial number, see the specific Installation Guide for your system.

End User License Agreement (EULA)

The first time a user logs into a Data Domain system, the End User License Agreement (EULA) is displayed. Customer acceptance is required, so an EMC representative should not accept the agreement.

If a customer is not present to accept the EULA, press **`Ctrl-C`** to exit from the EULA acceptance screen and continue the installation.

Later, you can instruct the customer to accept the EULA by using the DD System Manager, or by entering at the command-line interface (CLI):

```
# system show eula
```

CHAPTER 2

Using the CLI and DD System Manager Configuration Wizards

Introduction to the CLI and GUI Configuration Wizards

After you have completed installation, including powering on, enabling your console, and reviewing the EULA (end user license agreement), the CLI (command-line interface) Configuration Wizard will automatically start up, as described in the next sections.

After your initial configuration, you can again start up the CLI Configuration Wizard at any time, or you can use the Data Domain System Manager (GUI) Configuration Wizard, which is described later in this guide, to change or update your configuration.

Both wizards contain similar content, but the Data Domain System Manager Configuration Wizard provides some additional configuration options.

Run the Configuration Wizard

The CLI Configuration Wizard (a script) runs automatically the first time a Data Domain system is booted and can be run, as needed, by entering at the CLI (command-line interface):

```
# config setup
```

There is also a GUI Wizard that is part of the Data Domain System Manager, which is described in detail in the *EMC Data Domain Operating System Initial Configuration Guide*.

When you finish running the script, a reboot is *recommended*. If you have changed the time zone, a reboot is **required**.

As the script proceeds, you are prompted to answer a series of questions. Default values are contained in brackets immediately before the area for your input:

- Type **y** to answer yes.
- Type **n** to answer no.
- Press either the **Enter** or **Return** key to accept the given value, such as [mail], or type a new value.
- To make multiple entries in a list, separate each entry with either a comma or a space.
- When prompted for a hostname, enter either its IP address or its fully qualified domain name, such as srvr22.company.com.
- Be aware that you can run any command in the script at any time at the CLI.

At the end of the script, a summary of your entries is displayed. You can accept or reject your changes and exit to the CLI, or return to the beginning of that section and change any of the settings. When you select **Retry**, you will see your previous entries for each prompt.

To exit the script, you must have configured or skipped each of the sections, or you can enter **Ctrl+C**.

Running the CLI Configuration Wizard

Procedure

1. After you have logged into your system, you will see the CLI Configuration Wizard script start up automatically.
2. When asked if you want to use the GUI (Data Domain System Manager) wizard – if you enter **yes**, you will get a "short form" of the CLI wizard, and you can continue later with either the CLI wizard or the Data Domain System Manger (GUI) wizard. In order to go through the whole CLI wizard, this procedure will continue with **no**.

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

3. At this point, the script begins. You can configure or skip any section. The script automatically moves from one section to the next.

Configuring Licenses

Procedure

1. Licenses that you ordered with the Data Domain system are already installed.

   Type **yes** to configure or view licenses.

2. For each licensed feature, enter the license characters, including dashes.
3. For features not licensed, enter **no**, and press the **Enter** key.

   ```
   Licenses Configuration
            Configure Licenses at this time(yes|no) [no]: yes
   License Code
            Enter your license code
            : XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XX
            Do you want to add License (yes/no)?
            [no]: yes
   ```

4. A summary of your licenses appears. You can accept the settings (**Save**), reject the settings and exit to the command line (**Cancel**), or return to the beginning of the current section and change settings (**Retry**). A Retry shows your previous choice for each prompt. Press **Return** to accept the displayed value, or enter a new value.

   The license keys shown do not represent all possible keys on a system. If a key has not been installed at the factory, the license information should be contained with the shipping container.

   ```
   Pending License Settings
   CAPACITY-ACTIVE License   XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XX
   Do you want to save these settings (Save|Cancel|Retry): s

   Added "XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XX" : CAPACITY-ACTIVE feature
   for 21.8 TiB
   capacity ES30
   ```

Configuring the Network

Procedure

1. Type **yes** to configure the network.

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

2. Type **no** for the use of DHCP on any interface on the system.

```
Use DHCP
Use DHCP for hostname, domainname, default gateway and
DNS servers? (At least one interface needs to be configured
using DHCP)  (yes|no|?) [no]: no
```

3. Enter a fully qualified domain name (FQDN), for example – rstr01.yourcompany.com – for the hostname.

```
Hostname
Enter the hostname for this system (fully-qualified domain name)[]:
```

4. Enter a domain name, such as yourcompany.com.

   The system may be able to determine your domain name for you. Accept the entry if correct, or enter the correct value, and press **Enter** to proceed.

```
Domainname
Enter your DNS domainname []:
```

5. Configure the Ethernet interface designated as the IP address associated with the system hostname.

   This is typically the “management” interface, usually “ethMa”, but may be any interface. Skip configuration of other interfaces.

```
Ethernet port eth0a
Enable Ethernet port eth0a (yes|no|?) [yes]: no

Ethernet port eth0b
Enable Ethernet port eth0b (yes|no|?) [no]: yes

Use DHCP on Ethernet port eth0b (yes|no|?) [no]:

Enter the IP address for eth0b
[192.168.10.185]:

Enter the netmask for eth0b
[255.255.255.0]:
```

6. When not using DHCP on any Ethernet port, you must specify an IP address for a default routing gateway.

   If IPv6 is not in use, you may leave the “IPV6 Default Gateway” prompt empty.

```
Default Gateway
Enter the default gateway IP address
: 192.168.10.1
IPV6 Default Gateway
Enter the ipv6 default gateway IP address
:
```

7. When not using DHCP to acquire DNS servers, enter up to three DNS servers for a Data Domain system to use for resolving hostnames into IP addresses. Use a comma-separated or space-separated list. Enter a space for no DNS servers.

```
DNS Servers
Enter the DNS Server list (zero, one, two or three IP addresses)
: 192.168.10.1
```

8. A listing of your network settings appears. You can accept the settings (**Save**), reject the settings and exit to the command line (**Cancel**), or return to the beginning of the current section and change settings (**Retry**). A Retry shows your previous choice for each prompt. Press **Return** to accept the displayed value, or enter a new value.

```
Pending Network Settings
Hostname          ddbeta1.dallasrdc.com
```

```
Domain name       dallasrdc.com
Default Gateway   192.168.10.1
DNS Server List   192.168.10.1
Port       Enabled      Cable      DHCP      IP Address        Netmask or Prefix Length
-----      -------      -----      ----      --------------    ------------------------
eth0a      no           no         n/a       n/a               n/a
eth0b      no           no         n/a       n/a               n/a
eth0c      no           no         n/a       n/a               n/a
eth0d      no           no         n/a       n/a               n/a
ethMa      yes          yes        no        192.168.10.181    255.255.255.0
ethMb      no           no         n/a       n/a               n/a
ethMc      no           no         n/a       n/a               n/a
ethMd      no           no         n/a       n/a               n/a
ethMe      no           no         n/a       n/a               n/a
ethMf      no           no         n/a       n/a               n/a
-----      -------      -----      ----      --------------    ------------------------
Do you want to save these settings (Save|Cancel|Retry): save
```

9. The script will exit to the CLI with the following message displayed.

```
To complete this configuration in the Enterprise Manager,
please set your web browser address to http://<hostname_or_IP>/
then go to Maintenance -> More Tasks -> Launch Configuration
Wizard.
```

Configuring the File System

Procedure

1. Type **yes** to configure file system parameters. If the system has data-bearing disks in the chassis, a file system will already be present.

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

2. The next few questions relate to adding expansion shelves to the newly installed unit. Answer **no** to the following question. For systems that do not have expansion shelves, such as the DD2200, you will not see these entries.

```
Configure storage at this time (yes|no) [yes]: no
```

3. Enable the file system. These parameters should retain their default settings unless the person configuring the system has advanced knowledge of the implications.

```
Enable filesystem at this time (yes|no) [yes]: yes
Please wait.............
The filesystem is now enabled.
```

```
Global compression type
Will this restorer replicate to/from restorers with the old global
  compression type "1"? (yes|no|?) [no]:
Local compression type
What local compression type will this filesystem use? (none|lz|gz|
gzfast)
  [gz]: lz
Marker type
  What marker type will this filesystem use?
  (none|nw1|cv1|tsm1|tsm2|eti1|hpdp1|besr1|ssrt1|ism1|auto)
[auto]:

Pending Filesystem Settings
  Global Compression Type           9 (no change)
  Local Compression Type            lz
  Marker type                       auto
Do you want to save these settings (Save|Cancel|Retry): save
```

Configuring System Parameters

Procedure

1. Type **yes** to configure system parameters.

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

2. Add a client host from which you will administer the Data Domain system. The default NFS options are: rw, no_root_squash, no_all_squash, and secure. You can later use the commands `adminaccess add` and `nfs add /ddvar` to add other administrative hosts.

```
Admin host
  Enter a hostname for administrative access to the restorer
```

3. Add an email address so that someone at your site receives email for system alerts and autosupport reports, for example, **jsmith@yourcompany.com**. By default, the Data Domain system email lists include an address for the Data Domain support group. You can later use the Data Domain system commands `alerts` and `autosupport` to add more addresses.

```
Admin Email
  Enter an email address or group alias that will receive email
from the restorer.
```

4. Enter a location description for ease of identifying the physical machine. For example, **bldg4-rack10**. The alerts and autosupport reports display the location.

```
System Location
  Enter a physical location, to better identify this system.
```

5. Enter the name of a local SMTP (mail) server for Data Domain system emails. If the server is an Exchange server, be sure that SMTP is enabled.

```
SMTP Server
Enter the hostname of a mail (SMTP) server to relay email alerts.
[mail]
```

6. Enter your time zone. The default time zone for each Data Domain system is the factory time zone. For a complete list of time zones, refer to the appendix.

```
Timezone Name
  Enter your timezone name. [US/Pacific]:
```

7. (optional step) To allow the Data Domain system to use one or more Network Time Protocol (NTP) servers, you can enter IP addresses or server names. The default is to enable NTP and to use multicast. Be aware that the local time must be within a +/- 10000s variance to avoid a coredump of the ntp daemon on the Data Domain system.

```
Configure NTP
  Enable Network Time Service? (yes|no)|? [yes]:
  Use multicast for NTP? (yes|no) [yes]: no
  Enter the NTP Server list
  : 123.456.78.9
```

8. A listing of your network settings appears. You can accept the settings (**Save**), reject the settings and exit to the command line (**Cancel**), or return to the beginning of the current section and change settings (**Retry**). A Retry shows your previous choice for each prompt. Press **Return** to accept the displayed value, or enter a new value.

```
Pending System Settings
```

```
  Admin host          ddbeta7
  Admin email         jsmith@yourcompany.com
  system Location     bldg4-rack10
  SMTP Server         mail.yourcompany.com
  Timezone name       US/Pacific
  NTP Servers         123.456.78.9
  ---------------     --------------------
Do you want to save these settings (Save|Cancel|Retry):
```

Configuring the CIFS Protocol

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.

For information about EMC Data Domain MTrees, see the *EMC Data Domain DD OS Administrative Guide*.

To configure the CIFS protocol, type **yes**.

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

To specify CIFS clients that are allowed to access the `/ddvar` directory:

```
# cifs add /ddvar <client-list>
```

The `/ddvar` directory has the following subdirectories:

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

Configuring the NFS Protocol

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.

For information about EMC Data Domain MTrees, see the *EMC Data Domain DD OS Administrative Guide*.

To configure the NFS protocol, type **yes.**

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

Configuring VTL

Follow these steps to configure VTL. Ranges for all of the values you are to enter are shown, such as 1 - 32 characters for the name of the VTL.

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

Procedure

1. Create a VTL 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. 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 uppercase 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, enter0 so the value will be derived from the barcode.

   Table 3 Tape Codes, Capacities, and Types

Tape Code	Tape Capacity in GiB	Tape Type
L1	100	LT0-1
L2	200	LT0-2
L3	400	LT0-3
L4	800	LT0-4
LA	50	LT0-1
LB	30	LT0-1
LC	10	LT0-1

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.

```
Pending Settings
Library name    Knights
Changer model   TS3500
Slots           100
CAPs            1
Drive Model     IBM-LTO-3
Drives          2
Barcode         A99000LA
Capacity        0 (if 0, will be derived from barcode)
Group name      RoundTable
Initiators
------------------
pe2950_hba_zone_01
------------------
```

9. Review and save your settings.

Configuring DD Boost

For 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 Data Domain System Manager (GUI), which is described in the *EMC Data Domain Operating System Administration Guide*, or the `ddboost` command options, which are described in the *EMC Data Domain Operating System Command Reference Guide*.

Rebooting the Data Domain System

The CLI Configuration Wizard script will prompt for a reboot if the time zone has been changed. The reboot is mandatory before the time zone will be changed. For any other setting changes, a reboot is *suggested* as a best practice.

Procedure

1. To reboot the system, type:

```
# system reboot

The 'system reboot' command reboots the system. File access is
interrupted during the reboot.
Are you sure? (yes|no|?) [no]: yes

ok, proceeding.
The system is going down for reboot.
```

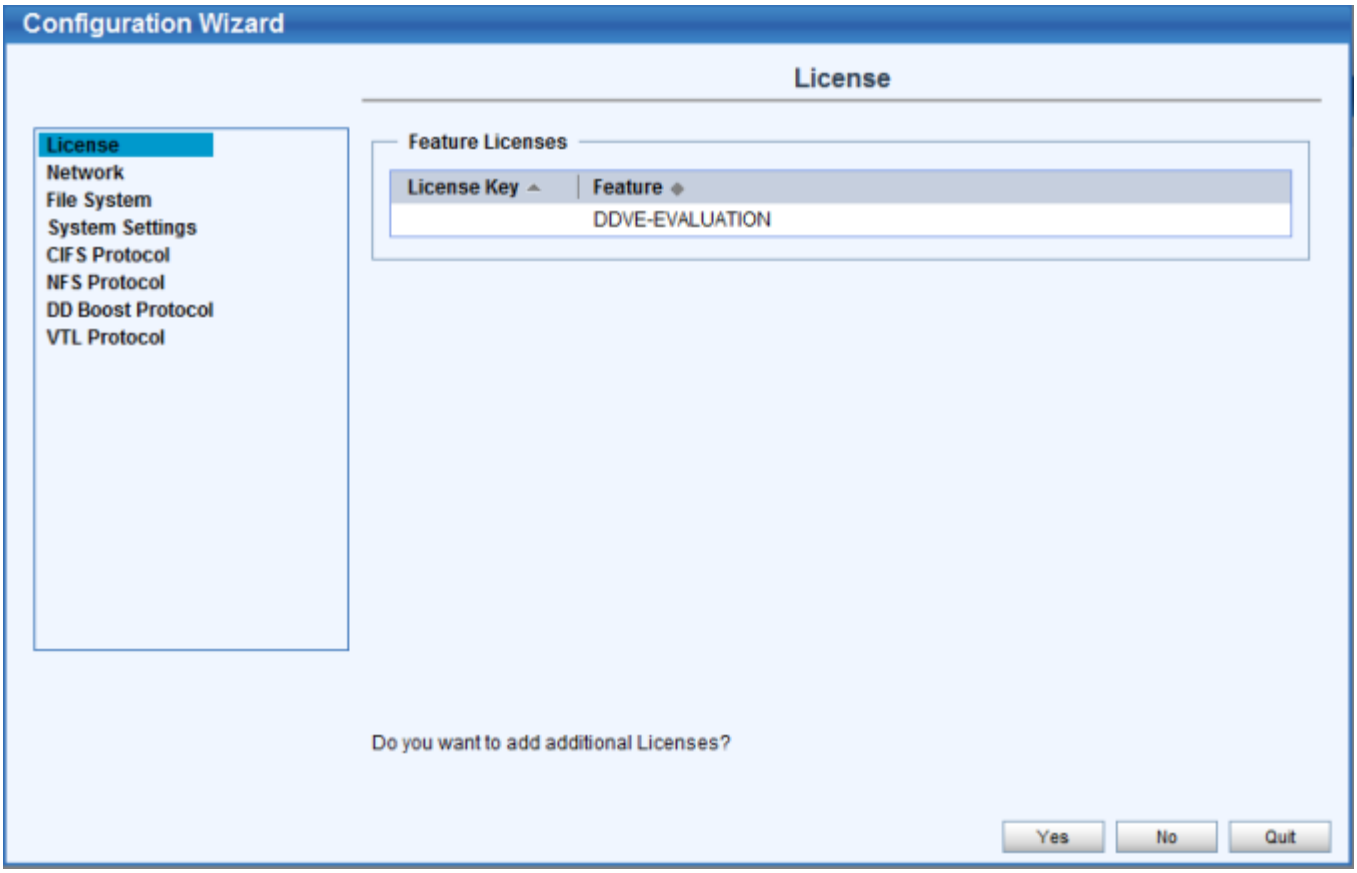
How to Use the Data Domain System Manager Configuration Wizard

Procedure

1. If this is the first time you have accessed the DD System Manager, open a web browser, and enter your Data Domain system's IP address in the browser's address text box. Wait for the DD System Manager to display the login screen. (If you have previously done this, see step 14.)
2. Enter your user name and password, and select **Login**.

The configuration modules are listed in the left pane. When one of the modules is selected, details are shown in the main pane. You can configure, or not configure, any module. However, you must start at the first module *Licenses* and either configure or skip every module in order, ending with *VTL Protocol*.

Figure 1 Data Domain System Manager Configuration Wizard



3. Move through the modules using the **Yes**, **No**, **Next**, and **Back** buttons.
4. **Licenses**: Enter your purchased license keys.
5. **Network**: Enter as follows:
   a. General: Either use DHCP or manually enter the hostname, domain name, and gateway IP address.
   b. Interfaces: Configure ports by using DHCP, or enter an IP address and netmask. Select DHCP's Enabled checkbox to enable the interface. When the interface is disabled, its settings cannot be changed.
   c. DNS information: DHCP or select an existing DNS IP address, or enter the DNS IP address.
6. **File System (DD Extended Retention and non-DD Extended Retention versions)**: Enter as follows:

   For *non-Data Domain Extended Retention* systems, enable the file system after creation.

   For *Data Domain Extended Retention* systems:

   a. Select whether to create a file system that supports Data Movement features and very large capacity. Be sure you want to create this kind of file system because it cannot be undone.

b. 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. Select the **Add to Tier** button, and select **Next.**

c. Select the size of the first Retention (Archive) Unit.

d. Select **Enable the file system after creation**.

7. **System Settings**: Set up the following to ensure that autosupport (ASUPs) and alert emails from your system are sent to Data Domain.

   a. 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.

   b. Mail Server. The name of the mail server used to send outgoing alert and autosupport emails to recipients. Recipients are subscribers to *groups*. A group named *default* is created with the email address of two subscribers: the administrator and autosupport-alert@autosupport.datadomain.com.

   c. Verify that the **Send Alert Notification Emails to Data Domain** is selected.

   d. Verify that the **Send Vendor Support Notification Emails to Data Domain** is selected.

   e. System Location. For your information only.

   f. Review the Summary page carefully. The default address for alerts and autosupport emails to Data Domain is `autosupport-alert @autosupport.datadomain`.com. The Vendor email is listed as Sending. The vendor email address, which cannot be changed, is `autosupport@autosupport.datadomain.com`

8. **CIFS Protocol**: Enter as follows:

   a. Workgroup: CIFS server name, if not using the default.

   b. Active Directory: Full realm name for the system, and a Domain Joining Credential user name and password.

   c. Optionally, Organizational Unit name, if not using the default.

   d. Share name and directory path.

   e. Client name, if not using the default.

9. **NFS Protocol**: Enter as follows:

   a. Pathname for the export.

   b. NFS client server name to be added to `/backup`, if not using an existing client. Select NFS options for the client. 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.

10. **DD Boost Protocol**: Enter as follows:

    a. (optionally) Change the Storage Unit name.

    b. Either select an existing user or create a new user by entering a user name, password, and minimum management role, which can be:

       - *backup (backup-operator)*: In addition to *user* privileges, lets you create snapshots, import and export tapes to a VTL, and move tapes within a VTL.
       - *None (none)*: Intended only for EMC DD Boost authentication, so you cannot monitor or configure a Data Domain system.

- *security (security)*: In addition to *user* privileges, lets you set up security-officer configurations and manage other security-officer operators.
- *sysadmin (admin)*: Lets you configure and monitor the entire Data Domain system.
- *user (user)*: Lets you monitor Data Domain systems and perform the `fastcopy` operation.

c. Select Next. If DD Boost is to be supported over Fibre Channel (FC), select the option to configure it.

d. Create an Access Group by entering a unique name. Duplicate access groups are not supported.

e. Select one or more initiators. Optionally, replace the initiator name by entering a new one. An initiator is a backup client that connects to the system to read and write data using the FC protocol. A specific initiator can support DD Boost over FC or VTL, but not both.

f. 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.

g. Select Next to review your changes, and select Submit when you are satisfied with your configuration.

11. **VTL Protocol**: Enter as follows:

a. Library name, number of drives, drive model, number of slots and CAPs, changer model name, starting barcode, and, optionally, tape capacity.

b. Create an Access Group. Enter a unique name. Duplicate access groups are not supported.

c. Select one or more initiators. Optionally, replace the initiator name by entering a new one. An initiator is a backup client that connects to a system to read and write data using the Fibre Channel protocol. A specific initiator can support EMC DD Boost over FC or VTL, but not both.

d. 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.

12. Use the **Quit** button to exit the wizard. For *help*, select the question mark in a dialog box.

13. After completing the wizard:

a. If you changed the date, time, or time zone, reboot the Data Domain system, as follows:

- Select the Data Domain system to be rebooted in the System Manager Navigation Pane.
- Select **Maintenance** › **System**.
- From the **More Tasks** menu, select **Reboot System**.
- Select **OK** at the Reboot System confirmation dialog box.

b. Complete the post-configuration tasks in Post-Configuration Setup on page 23.

14. To return to the wizard to reconfigure any modules from within the DD System Manager, select 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.

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:

Verifying Network Connectivity

After you have completed your core setup and rebooted your system (if needed), you should verify your network connectivity.

Procedure

1. Type:

```
# ssh sysadmin@hostname
```

2. Ping the default gateway.

```
# ping <gateway ip address>
```

Setting up, Testing, and Getting Autosupports

A Data Domain system sends out two emails each day: an autosupport email and an alert summary email. In addition, if an alert event occurs, an alert event email is generated.

The autosupport email contains device state and configuration items. The alert summary email contains current alerts, alerts history, and log messaging. The alert event email contains alert notifications as they occur.

By default, the email lists, which are comma-separated, space-separated, or both, include addresses for Data Domain support staff. To add an email address to any email list, use the `autosupport add` or `alerts add` commands.

Procedure

1. To add addresses to the autosupport email list, enter:

```
# autosupport add asup-detailed emails test@test.com

Autosupport email:

autosupport@autosupport.datadomain.com
east1dd510a@datadomain.com
test@test.com
```

2. To add addresses to the alert summary email list, enter:

```
# autosupport add alerts-summary emails test@test.com

Alerts summary email:

autosupport@autosupport.datadomain.com
east1dd510a@datadomain.com
test@test.com
```

3. To add addresses to the alert event email list, enter:

```
# alerts notify-list add emails test@test.com

Alerts email:

autosupport-alert@autosupport.datadomain.com
east1dd510a@datadomain.com
test@test.com
```

4. Create further support lists, as needed.

5. Customer external mail relays must be configured to allow emails generated by the Data Domain system to exit the network from which it is currently attached. To test that external mail relays allow this, enter:

```
# autosupport test email jsmith@yourcompany.com

OK: Message sent.
```

   If the result is `OK: message sent`, then the mail has been forwarded outside of the current network and should be working. If an error message is generated, ask the client to verify mail relay settings. In the field, the best way to confirm this is to add yourself to the test line and verify that the test email arrives at your email-enabled mobile device.

6. To get an autosupport file off of a Data Domain system, there are two methods. In order of preference, they are:

   - Using an `autosupport send` command where the Implementation Specialist is the recipient using the following command:

     ```
     # autosupport send example_user@emc.com
     ```

   - By logging into the /ddvar/support directory and retrieving it from that location.

   The first method is preferred because, as part of the normal installation and testing process above, autosupports must be sent to autosupport@autosupport.datadomain.com. After that is done, sending an additional autosupport takes moments. The other two methods are included in case it is impossible to get the autosupports relaying out of the customer environment to the Data Domain support staff.

Configuring 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 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:

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

CHAPTER 4

Additional Configuration Procedures

This chapter describes some additional configuration procedures that are performed after initial configuration with the Configuration Wizard is complete.

This chapter covers the following topics:

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 will display an error message that the network name no longer exists.

On all CIFS backup servers that use a Data Domain system, it is a good practice to change the session time-out parameter to 1800 (30 minutes), as described in the following procedure.

Changing the Default Timeout Value

Procedure

1. On a Windows machine, select **Start** › **Run** and type `REGEDT32` in the **Open:** text box.
2. Select **OK.**
3. In the Registry Editor dialog, if it is not already expanded, click `Computer` 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. **For Windows 2003 R2 Servers**, look for a `SESSTIMEOUT` key. [If you do not see it, right-click within an empty space in the right pane, select **New** › **Key**, and name the new key `SESSTIMEOUT`, using all caps.] Double-click the `SESSTIMEOUT` key, and set its value to 1800 (30 minutes).
6. **For Windows 2008 R8 Servers**, look for an `ExtendedSessTimeout` registry parameter. [If you do not see it, add it with type `REG_DWORD`.] Set the `ExtendedSessTimeout` registry parameter to 1800 (30 minutes). Then, look for a `ServersWithExtendedSessTimeout` registry parameter. [If you do not see it, add it with type `REG_MULT_SZ`.] Set the `ServersWithExtendedSessTimeout` registry parameter to the list of one or more Data Domain servers, where each server is either an IP address or the name of the Data Domain system. If you use different names or use both IP address and name for a given Data Domain system, all of them must be included here.

Advanced Network Configuration

You can configure three additional advanced network features on a Data Domain system:

- Ethernet Failover
  You can configure multiple network interfaces on a Data Domain system to function as a single virtual interface. If a network interface configured as part of a virtual interface fails, network activity switches to another port. Ethernet failover provides improved network stability. For more information, see the sections on Failover in the *EMC DD OS Administration Guide* and the *EMC DD OS Command Reference Guide*.
- Link Aggregation
  You can use multiple physical Ethernet network ports in parallel, which increases link speed and also provides a reduced performance failover capability that is better than a single port. For more information, see the sections on Link Aggregation in the *EMC DD OS Administration Guide* and the *EMC DD OS Command Reference Guide*.
- VLAN Tagging
  You can set an interface on a Data Domain system to support multiple IEEE 802.1Q VLANs, with an interface configured with a distinctive VLAN IP address. You must

configure the switch that connects to the interface to send data from multiple VLANs to the Data Domain system, using the proper VLAN encapsulation, as specified by the 802.1Q protocol. For more information, see the sections on VLAN in the *EMC DD OS Administration Guide* and the *EMC DD OS Command Reference Guide*.

Understanding Ethernet Port-Naming Conventions

The Ethernet port-naming convention for all Data Domain systems shipped before DD OS 4.9 included only a number for each port, without consideration for the physical location of that port (for example, eth0 to eth5).

Starting with systems shipped with DD OS 4.9, the Ethernet interface-naming scheme refers to 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 get information about ports on a 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.

Creating Virtual Interfaces

To create virtual interfaces for failover or link aggregation, use pairs supported for the type of interface you are creating – being aware that:

- 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 fibre, 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.

To create a virtual interface:

Procedure

1. Type:

   ```
   # net create virtual vethx
   ```

   where *x* is the variable for the virtual name, which must begin with veth. The variable consists of decimal or hexadecimal numbers (0-9 and aA-fF) that serve as a unique identifier for the virtual interface.

2. Type:

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

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

Configuring Failover

Use the on-board port ethMa only for maintenance. Do not bond it with optional card ports. This may not apply to all Data Domain systems.

To configure failover:

Procedure

1. Create a virtual interface and assign it an IP address. For instructions, see the previous section on creating virtual interfaces.
2. Disable each of the Ethernet ports *ifname* that are to be part of the virtual interface by entering (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.

   ```
   # 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:

   ```
   # 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:

   ```
   # 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:

   ```
   # 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:

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

Configuring Link Aggregation

The `net aggregate` command enables a virtual interface for link aggregation with the specified physical interfaces.
You must select one of the following aggregation modes because there is no default. The mode must be compatible with the switch in use.

- roundrobin
  Transmits packets sequentially, from the first available link through the last in the aggregated group.
- balanced
  Sends data over interfaces as determined by the hash method selected. This requires the associated interfaces on the switch to be grouped into an Ethernet truck. Requires a hash.
- lacp
  Communicates with the other end, based on LACP (Link Aggregation Control Protocol, IEEE 802.3ad), to coordinate which links within the bond are available. Both ends must be configured with LACP to use this mode.
- xor-L2
  Transmits packets, based on static balanced or LACP mode, with an XOR hash of Layer 2 (inbound and outbound MAC addresses).
- xor-L2L3
  Transmits packets, based on static balanced or LACP mode, with an XOR hash of Layer 2 (inbound and outbound MAC addresses) and Layer 3 (inbound and outbound IP addresses).
- xor-L3L4
  Transmits packets, based on static balanced or LACP mode, with an XOR hash of Layer 3 (inbound and outbound IP address) and Layer 4 (inbound and outbound port numbers).

Here are some additional considerations before configuring link aggregation:

- 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.
- The Akula NIC cannot be used for customer data.
- You can configure two or more Ethernet ports as interfaces for link aggregation.
- A physical port cannot already have been 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.

Here is how to configure link aggregation:

Procedure

1. Create a virtual interface, and assign it an IP address. For more information, see the previous section on creating virtual interfaces.
2. Disable each of the physical ports that you plan to use as aggregation interfaces, by entering:

```
# 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 (mode must be specified the first time):

```
# net aggregate add virtual-ifname interfaces physcial-ifname-list
[mode {roundrobin | balanced hash {xor-L2 | xor-L3L4 | xor-L2L3 }
| lacp hash
{xor-L2 | xor-L3L4 | xor-L2L3 }
```

For example, to enable link aggregation on virtual interface veth1 to physical interfaces eth1a and eth2a in mode lacp hash xor-L2:

```
 # net aggregate add veth1 interfaces eth1a eth2a mode lacp hash
xor-L2
```

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

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

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:

```
# net aggregate show
```

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

Configuring VLAN Tagging

To configure VLAN tagging:

Procedure

1. Configure the switch port connected to the interface that is to receive and send VLAN traffic from the Data Domain interface. (For configuration information, see your specific switch documentation.)
2. On the Data Domain system, enable the interface that you plan to use as the VLAN interface, for example, *eth5b*:

```
# net config eth5b up
```

3. Create the VLAN interface using either a physical port or a configured virtual port (for the latter, see the previous section on creating virtual interfaces):

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

where the range for *vlan-id* is between 1 and 4094 inclusive. For example, to create a VLAN interface, named eth5b.1, on a physical interface *eth5b*:

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

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 (which is *eth5b.1* in this example), *ipaddr* is the interface's IP address, and *mask* is the corresponding netmask. Be aware that DHCP cannot be used to assign an IP address to a VLAN.

5. Verify that the interface has been created:

```
# net show settings

port     enabled   DHCP   IP address       netmask          type
additional setting
                                           /prefix length
------   -------   ----   --------------   --------------   ----
------------------
eth5b1   yes       yes    192.168.8.175*   255.255.252.0    n/a
```

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

Additional Physical or Virtual Interface Configuration

You can set auto-negotiate for an interface, specify the maximum transfer unit (MTU) size, and configure duplex line usage and speed, as described in the following sections.

Setting Auto-Negotiate for an Interface

To set auto-negotiate for an interface, enter:

```
# net config ifname autoneg
```

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

```
# net config eth1a autoneg
```

Specifying the MTU Size

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

To specify the MTU size, enter:

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

where *ifname* is the name of the interface.

Configuring Duplex Line Use and Speed

To configure duplex line use and speed for an interface, use one of these 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.

Here are a few restrictions to note:

- 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
```

Configuring SNMP on a Data Domain System

From an SNMP perspective, a Data Domain system is a read-only device with one exception: a remote machine can set the SNMP location, contact, and system name on a Data Domain system.

The `snmp` command lets you configure community strings, hosts, and other SNMP variables on a Data Domain system.

With one or more trap hosts defined, a Data Domain system also sends alert messages as SNMP traps, even when the SNMP agent is disabled.

Displaying Configuration Commands

To view the current SNMP configuration, enter:

```
# snmp show config
```

Adding a Community String

As an administrator, enter one of these commands to 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
```

Enabling SNMP

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

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.

Setting the System Location

As an administrator, enter:

```
# snmp set sysLocation location
```

This sets the system location, as used in the SNMP MIB II system variable `sysLocation`. For example:

```
# snmp set sysLocation bldg3-rm222
```

Setting a System Contact

As an administrator, enter:

```
# snmp set sysContac contact
```

This 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 SNMP variables are not set with `snmp` commands, the variables default to the system values given as part of the `config set` commands.

Adding a Trap Host

As an administrator, enter:

```
# snmp add trap-host host-name-list[:port [version {v2c | v3 }]
community community | user 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 adds a trap host to the list of machines that receive SNMP traps generated by a 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 lets you view the serial output of a remote system's boot sequence. See the *EMC Data Domain Operating System Command Reference Guide* for how to configure SOL for IPMI.

Configuring Encryption for Data at Rest

The optional *Encryption for Data at Rest* feature encrypts all incoming data before writing it to a 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.

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.

See the *EMC Data Domain Operating System Administration Guide* for more about this feature and to view related configuration and management procedures.

Optional Configuration Procedures

At this point, you can perform the following tasks, or you can do them later on.

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

- 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

CHAPTER 5

Adding Expansion Shelves

This chapter covers the following topics:

Adding an Expansion Shelf

To install a new expansion shelf, see the *Data Domain Expansion Shelf Hardware Guide* for your shelf model or models.

The following procedure, which adds an enclosure to the volume and creates RAID groups, applies only to adding a shelf to the active tier of a Data Domain system. For adding a shelf to a system with the Extended Retention feature, see the appropriate *Data Domain Expansion Shelf Hardware Guide* and the *EMC Data Domain Operating System Administration Guide*.

A 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.

NOTICE

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 the EMC Online Support Site.

Adding an Enclosure to the Volume

To add an enclosure to the volume:

Procedure

1. For each enclosure that you want to add, enter:

   ```
   # 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. The EMC Data Domain controller always has enclosure-id of 1 (one).
2. When prompted, enter your sysadmin password.
3. (optional) Add disks in another enclosure at this time, also using the `storage add` command.
4. Display the RAID groups for each shelf:

   ```
   # storage show all
   ```

   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.

Making Disks Labeled Unknown Usable to the System

To make a disk labeled unknown usable to the system, follow these steps. This is not part of a standard initialization; it is included here only for troubleshooting purposes.

Procedure

1. For each unknown disk, enter:

   ```
   # disk unfail
   ```

   For example, if two disks 2.15 and 2.16 are labeled unknown:

   ```
   # disk unfail 2.15
   # disk unfail 2.16
   ```

2. Verify the new state of the file system and disks:

   ```
   # filesys status
   ```

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

   ```
   # filesys show space
   ```

Verifying Shelf Installation

To verify shelf installation:

Procedure

1. After installing new shelves, check the status of the SAS HBA cards:

   ```
   # 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:

   ```
   # 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.

APPENDIX A

Time Zones

This appendix covers the following topics:

Time Zones Overview

Time zones are used to establish your location when you initially configure your system.

Locate your time zone using the following tables.

A time zone can consist of two entries separated by a slash (/). The first entry can be a continent, nation, or region, such as Africa, the Pacific, or the United States. The second entry is the city closest to you within that area.

A time zone, and some miscellaneous entries such as GMT, Cuba, and Japan, can also be a single entry.

Examples of time zones include:

- Indiana/Indianapolis
- GMT+5
- Stockholm
- Pacific
- EasterIsland
- Japan

Africa

Abidjan	Accra	Addis_Ababa	Algiers	Asmara
Asmera	Bamako	Bangui	Banjul	Bissau
Blantyre	Brazzaville	Bujumbura	Cairo	Casablanca
Ceuta	Conakry	Dakar	Dar_es_Salaam	Djibouti
Douala	El_Aaiun	Freetown	Gaborone	Harare
Johannesburg	Juba	Kampala	Khartoum	Kigali
Kinshasa	Lagos	Libreville	Lome	Luanda
Lubumbashi	Lusaka	Malabo	Maputo	Maseru
Mbabane	Mogadishu	Monrovia	Nairobi	Ndjamena
Niamey	Nouakchott	Ouagadougou	Porto-Novo	Sao_Tome
Timbuktu	Tripoli	Tunis	Windhoek	

America

Adak	Anchorage	Anguilla	Antigua	Araguaina
Argentina/ Buenos_Aires	Argentina/ Catamarca	Argentina/ ComoRivadavia	Argentina/ Cordoba	Argentina/Jujuy
Argentina/ La_Rioja	Argentina/Mendoza	Argentina/ Rio_Gallegos	Argentina/Salta	Argentina/ San_Juan

Argentina/ San_Luis	Argentina/Tucuman	Argentina/Ushuaia	Aruba	Asuncion
Atikokan	Atka	Bahia	Bahia_Banderas	Barbados
Belem	Belize	Blanc-Sablon	Boa_Vista	Bogota
Boise	Buenos_Aires	Cambridge_Bay	Campo_Grande	Cancun
Caracas	Catamarca	Cayenne	Cayman	Chicago
Chihuahua	Coral_Harbour	Cordoba	Costa_Rica	Creston
Cuiaba	Curacao	Danmarkshavn	Dawson	Dawson_Creek
Denver	Detroit	Dominica	Edmonton	Eirunepe
El_Salvador	Ensenada	Fort_Wayne	Fortaleza	Glace_Bay
Godthab	Goose_Bay	Grand_Turk	Grenada	Guadeloupe
Guatemala	Guayaquil	Guyana	Halifax	Havana
Hermosillo	Indiana/ Indianapolis	Indiana/Knox	Indiana/ Marengo	Indiana/ Petersburg
Indiana/ Tell_City	Indiana/Vevay	Indiana/Vincennes	Indiana/ Winamac	Indianapolis
Inuvik	Iqaluit	Jamaica	Jujuy	Juneau
Kentucky/ Louisville	Kentucky/ Monticello	Knox_IN	Kralendijk	La_Paz
Lima	Los_Angeles	Louisville	Lower_Princes	Maceio
Managua	Manaus	Marigot	Martinique	Matamoros
Mazatlan	Mendoza	Menominee	Merida	Metlakatla
Mexico_City	Miquelon	Moncton	Monterrey	Montevideo
Montreal	Montserrat	Nassau	New_York	Nipigon
Nome	Noronha	North_Dakota/ Beulah	North_Dakota/ Center	North_Dakota/ New_Salem
Ojinaga	Panama	Pangnirtung	Paramaribo	Phoenix
Port-au-Prince	Port_of_Spain	Porto_Acre	Porto_Velho	Puerto_Rico
Rainy_River	Rankin_Inlet	Recife	Regina	Resolute
Rio_Branco	Rosario	Santa_Isabel	Santarem	Santiago
Santo_Domingo	Sao_Paulo	Scoresbysund	Shiprock	Sitka
St_Barthelemy	St_Johns	St_Kitts	St_Lucia	St_Thomas
St_Vincent	Swift_Current	Tegucigalpa	Thule	Thunder_Bay
Tijuana	Toronto	Tortola	Vancouver	Virgin
Whitehorse	Winnipeg	Yakutat	Yellowknife	

Antarctica

Casey	Davis	DumontDUrville	Macquarie	Mawson
McMurdo	Palmer	Rothera	South_Pole	Syowa
Troll	Vostok			

Asia

Aden	Almaty	Amman	Anadyr	Aqtau
Aqtobe	Ashgabat	Ashkhabad	Baghdad	Bahrain
Baku	Bangkok	Beijing	Beirut	Bishkek
Brunei	Calcutta	Chita	Choibalsan	Chongqing
Chungking	Colombo	Dacca	Damascus	Dhaka
Dili	Dubai	Dushanbe	Gaza	Harbin
Hebron	Ho_Chi_Minh	Hong_Kong	Hovd	Irkutsk
Istanbul	Jakarta	Jayapura	Jerusalem	Kabul
Kamchatka	Karachi	Kashgar	Kathmandu	Katmandu
Khandyga	Kolkata	Krasnoyarsk	Kuala_Lumpur	Kuching
Kuwait	Macao	Macau	Magadan	Makassar
Manila	Muscat	Nicosia	Novokuznetsk	Novosibirsk
Omsk	Oral	Phnom_Penh	Pontianak	Pyongyang
Qatar	Qyzylorda	Rangoon	Riyadh	Saigon
Sakhalin	Samarkand	Seoul	Shanghai	Singapore
Srednekolymsk	Taipei	Tashkent	Tbilisi	Tehran
Tel_Aviv	Thimbu	Thimphu	Tokyo	Ujung_Pandang
Ulaanbaatar	Ulan_Bator	Urumqi	Ust-Nera	Vientiane
Vladivostok	Yakutsk	Yekaterinburg	Yerevan	

Atlantic

Azores	Bermuda	Canary	Cape_Verde	Faeroe
Faroe	Jan_Mayen	Madeira	Reykjavik	South_Georgia
St_Helena	Stanley			

Australia

ACT	Adelaide	Brisbane	Broken_Hill	Canberra
Currie	Darwin	Eucla	Hobart	LHI
Lindeman	Lord Howe	Melbourne	NSW	North
Perth	Queensland	South	Sydney	Tasmania
Victoria	West	Yancowinna		

Brazil

Acre	DeNoronha	East	West

Canada

Atlantic	Central	East-Saskatchewan	Eastern
Mountain	Newfoundland	Pacific	Saskatchewan
Yukon			

Chile

Continental	EasterIsland

Etc

GMT	GMT+0	GMT+1	GMT+2	GMT+3
GMT+4	GMT+5	GMT+6	GMT+7	GMT+8
GMT+9	GMT+10	GMT+11	GMT+12	GMT0
GMT-0	GMT-1	GMT-2	GMT-3	GMT-4
GMT-5	GMT-6	GMT-7	GMT-8	GMT-9
GMT-10	GMT-11	GMT-12	GMT-13	GMT-14
Greenwich	UCT	Universal	UTC	Zulu

Europe

Amsterdam	Andorra	Athens	Belfast	Belgrade

Berlin	Bratislava	Brussels	Bucharest	Budapest
Busingen	Chisinau	Copenhagen	Dublin	Gibraltar
Guernsey	Helsinki	Isle_of_Man	Istanbul	Jersey
Kaliningrad	Kiev	Lisbon	Ljubljana	London
Luxembourg	Madrid	Malta	Mariehamn	Minsk
Monaco	Moscow	Nicosia	Oslo	Paris
Podgorica	Prague	Riga	Rome	Samara
San_Marino	Sarajevo	Simferopol	Skopje	Sofia
Stockholm	Tallinn	Tirane	Tiraspol	Uzhgorod
Vaduz	Vatican	Vienna	Vilnius	Volgograd
Warsaw	Zagreb	Zaporozhye	Zurich	

GMT

GMT	GMT+1	GMT+2	GMT+3	GMT+4
GMT+5	GMT+6	GMT+7	GMT+8	GMT+9
GMT+10	GMT+11	GMT+12	GMT+13	GMT-1
GMT-2	GMT-3	GMT-4	GMT-5	GMT-6
GMT-7	GMT-8	GMT-9	GMT-10	GMT-11
GMT-12				

Indian (Indian Ocean)

Antananarivo	Chagos	Christmas	Cocos	Comoro
Kerguelen	Mahe	Maldives	Mauritius	Mayotte
Reunion				

Mexico

BajaNorte	BajaSur	General

Miscellaneous

Arctic/ Longyearbyen	CET	CST6CDT	Cuba	EET

Egypt	Eire	EST	EST5EDT	Factory
GB	GB-Eire	Greenwich	Hongkong	HST
Iceland	Iran	Israel	Jamaica	Japan
Kwajalein	Libya	MET	MST	MST7MDT
Navajo	NZ	NZ-CHAT	Poland	Portugal
PRC	PST8PDT	ROC	ROK	Singapore
Turkey	UCT	Universal	UTC	WET
W-SU	Zulu			

Pacific

Apia	Auckland	Chatham	Chuuk	Easter
Efate	Enderbury	Fakaofo	Fiji	Funafuti
Galapagos	Gambier	Guadalcanal	Guam	Honolulu
Johnston	Kiritimati	Kosrae	Kwajalein	Majuro
Marquesas	Midway	Nauru	Niue	Norfolk
Noumea	Pago_Pago	Palau	Pitcairn	Pohnpei
Ponape	Port_Moresby	Rarotonga	Saipan	Samoa
Tahiti	Tarawa	Tongatapu	Truk	Wake
Wallis	Yap			

US (United States)

Alaska	Aleutian	Arizona	Central	East-Indiana
Eastern	Hawaii	Indiana-Starke	Michigan	Mountain
Pacific	Pacific-New	Samoa		

Aliases

GMT=Greenwich, UCT, UTC, Universal, Zulu CET=MET (Middle European Time)
Eastern=Jamaica Mountain=Navajo