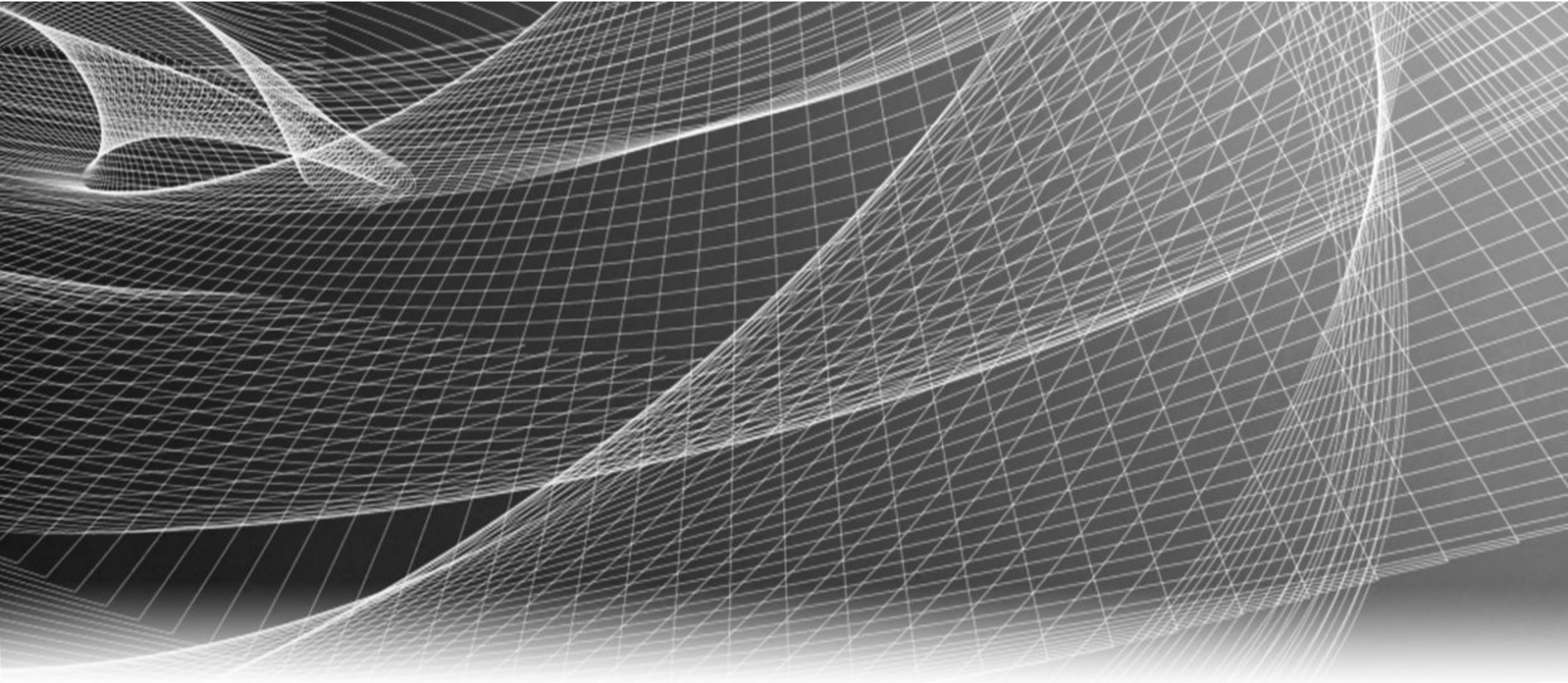


EMC® Data Domain® Operating System

Version 5.6

Initial Configuration Guide

302-001-634

REV 01

Published April, 2015

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided as is. EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date regulatory document for your product line, go to EMC Online Support (https://support.emc.com).

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

CONTENTS

Preface 5

Revision history 7

Chapter 1 Before Starting Configuration 9

Powering on all systems 10
Enabling administrative communication 10
Accepting the End User License Agreement (EULA) 11
Changing the password 11

Chapter 2 CLI Configuration Wizard 13

Getting started with the CLI Configuration Wizard 14
Configuring licenses 15
Configuring the network 15
Configuring the file system 17
Configuring system parameters 17
Configuring the CIFS protocol 19
Configuring the NFS protocol 19
Configuring VTL 19
Configuring DD Boost 21
Rebooting a Data Domain system 21

Chapter 3 Data Domain System Manager Configuration Wizard 23

Getting started with the DD System Manager Configuration Wizard 24
Using the DD System Manager Configuration Wizard 25

Chapter 4 Post-Configuration Setup 29

Verifying network connectivity 30
Setting up, testing, and getting autosupports 30
Setting up ConnectEMC 31
Configuring security and firewalls (NFS and CIFS access) 32

Chapter 5 Additional Configuration Procedures 37

Changing the timeout on CIFS backup servers 38
- Changing the default timeout value 38

Advanced network configuration 38
- Understanding Ethernet port-naming conventions 39
- Creating virtual interfaces 39
- Configuring failover 40
- Configuring link aggregation 41
- Configuring VLAN tagging 42
- Additional physical or virtual interface configuration 43

Configuring SNMP on a Data Domain system 43
- Displaying configuration commands 44
- Adding a community string 44
- Enabling SNMP 44

Setting the system location 44
Setting a system contact 44
Adding a trap host 44
Configuring SOL for IPMI 45
Configuring Encryption for Data at Rest 45
Optional configuration procedures 45

Chapter 6 Adding Expansion Shelves 47

Adding an expansion shelf 48
Adding enclosure disks to the volume 48
Making disks labeled unknown usable to the system 49
Verifying shelf installation 49

Appendix A Time Zones 53

Time zones overview 54
Africa 54
America 54
Antarctica 56
Asia 56
Atlantic 57
Australia 57
Brazil 57
Canada 57
Chile 58
Etc 58
Europe 58
GMT 59
Indian (Indian Ocean) 59
Mexico 59
Miscellaneous 59
Pacific 60
US (United States) 60
Aliases 60

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 post-installation 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 post-installation 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 the *EMC Data Domain Initial Configuration 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:

NOTICE

Identifies content that warns of potential business or data loss.

Note

Contains information that is incidental, but not essential, to the topic.

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

Table 2 Revision history

Revision	Date	Description
01	April 2015	Initial publication for release 5.6. Updates include: • There is a new notification that you may be locked out for 120 seconds if you enter an incorrect password 4 consecutive times. See *Enabling administrative communication*. • There is a change to the login procedure. See *Enabling administrative communication*. • A new section on ConnectEMC has been added. See *Setting up ConnectEMC*.

CHAPTER 1

Before Starting Configuration

This chapter describes the steps you must complete before starting configuration, if you have not completed them already. Most of these steps are also covered in your specific *EMC Data Domain Operating System Installation and Setup Guide*.

- Powering on all systems 10
- Enabling administrative communication 10
- Accepting the End User License Agreement (EULA) 11
- Changing the password 11

Powering on all systems

You must first power on all expansion shelves, if applicable, before powering on the controller.

1. Power on all expansion shelves, if applicable.
2. Again, if applicable, let the shelves reach a stable state by waiting approximately 3 minutes.
3. Connect the controller to a power source. Most systems power on when plugged in; some also have a power button.

   Note

   Data Domain systems should be powered on from redundant AC sources. Check your specific *EMC Data Domain Operating System Setup and Installation Guide*.

Enabling administrative communication

After you have powered on your system, you must set up and log into an administrative console to enable communication.

Procedure

1. Connect an administrative console to the serial connection at the location appropriate for your Data Domain system.
2. Launch a terminal emulation program from your computer, and configure the communication settings. For the settings for a particular DD system, consult the appropriate *EMC Data Domain Operating System Installation and Setup Guide*.
3. If you do not see a prompt, press Enter. If you still do not see a prompt, check the power light. If the power light is off, for some DD systems, you must press a power button.
4. Log into the Data Domain CLI (command-line interface) as user **sysadmin**.

   ```
   localhost.localdomain login: sysadmin
   ```

5. Enter the default password, which is the system serial number (SSN). If you cannot find it, consult the appropriate *EMC Data Domain Operating System Installation and Setup Guide*.

   ```
   password: <system_serial_number>
   ```

   Note

   If you enter an incorrect password 4 consecutive times, the system locks out the specified username for 120 seconds. The login count and lockout period are configurable, but these are the defaults, which you will get during an initial configuration. To configure these values, see the *EMC Data Domain Operating System Administration Guide* and the *EMC Data Domain Operating System Command Reference Guide*.

Accepting the End User License Agreement (EULA)

The first time you log in to a Data Domain system, the End User License Agreement (EULA) is displayed.

At the end of the EULA, you are prompted to accept it:

```
Press any key then hit enter to acknowledge the receipt of EULA
information
```

Note

The EULA *must* be accepted by a customer. An EMC representative should *not* accept this agreement. If a customer is not present, press **`Ctrl-C`** to exit from the EULA acceptance screen and continue the installation.

The customer can later enter the following to redisplay the EULA and accept it:

```
system show eula
```

Changing the password

If the EULA has been accepted, you will see the following password change prompt, to which you should answer **`yes`** and change the password.

```
Change the 'sysadmin' password at this time? (yes|no): yes
```

Note

If you are an EMC representative, do not change the password unless specifically directed to do so by the customer.

CHAPTER 2

CLI Configuration Wizard

- Getting started with the CLI Configuration Wizard 14
- Configuring licenses 15
- Configuring the network 15
- Configuring the file system 17
- Configuring system parameters 17
- Configuring the CIFS protocol 19
- Configuring the NFS protocol 19
- Configuring VTL 19
- Configuring DD Boost 21
- Rebooting a Data Domain system 21

Getting started with the CLI Configuration Wizard

The CLI Configuration Wizard (a script) runs automatically the first time you boot-up a Data Domain system.

Note

This script will run every time you login until your “firstboot” process (acceptance of the EULA and a total run-through of the CLI Configuration Wizard) is successfully completed. Therefore, if you simply use `Ctrl+C` to exit the wizard, you will not have “completed” the wizard, and it will be reactivated each time you login.

The script automatically moves from one section to the next, and 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, and then press either the `Enter` or `Return` key.
- To make multiple entries in a list, separate each entry with either a comma or a space.
- When prompted for a host name, 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 CLI Configuration Wizard at any time at the CLI.

At the end of each section, 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.

Note

If you have exited the script, you can re-start it at any time by entering:

```
# config setup
```

Procedure

1. Enter `no` to start the complete CLI Configuration Wizard.

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

   Note

   The initial prompt gives you the option of using a *shortened* version of the CLI Configuration Wizard that provides only enough information to configure the system for network access [and then directs you to the Data Domain System Manager (GUI) Configuration Wizard]. For this chapter, the assumption is that you will answer “no” at this point. However, if you want to use the Data Domain System Manager (GUI) Configuration Wizard, answer “yes”, go through the *Configuring the Network* section, and then skip to the *Data Domain System Manager Configuration Wizard* chapter.

2. Continue to the next sections to configure licenses, the network, the file system, system parameters, the CIFS protocol, the NFS protocol, VTL, and/or DD Boost.

Configuring licenses

Procedure

1. The licenses that you ordered with your 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
         : C97H-PTRP-7328-4HU2-KDJE

         Do you want to add License (yes/no)?
         [no]:
```

4. A summary of the licenses that you just added 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
I/OS License   C97H-PTRP-7328-4HU2-KDJE
         Do you want to save these settings (Save|Cancel|Retry):
```

Configuring the network

Procedure

1. Enter **yes** to configure the system for network connectivity.

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

2. Enter **yes** to configure DHCP (Dynamic Host Configuration Protocol) to obtain network parameters (such as, the host name, domain name, and IP addresses) dynamically from a DHCP server. Or enter **no** to configure the parameters manually.

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

3. Enter a fully qualified domain name (FQDN) for the host name; for example, **str01.yourcompany.com**. Or accept the host name, if the system was able to discover it.

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

4. Enter the DNS (Domain Name System) domain name; for example, **`yourcompany.com`**. Or accept the domain name, if the system was able to discover it.

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

5. Enable and configure each Ethernet interface. Accept or decline DHCP for each interface. If the port does not use DHCP to discover network parameters automatically, enter the information manually.

```
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. Enter the IP address of the default routing gateway. Or accept the default gateway, if the system was able to discover it.

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

7. Enter the IPv6 address of the default routing gateway. Or accept the IPv6 address of the default gateway, if the system was able to discover it. If IPv6 is not in use, leave the field empty, and press **`Enter`** to continue.

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

8. Enter up to three DNS servers to use for resolving host names to IP addresses. Use a comma-separated or space-separated list. Enter a space for no DNS servers. Or accept the IP addresses of the DNS servers, if the system was able to discover them.

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

9. A summary of the network settings is displayed. You can accept the settings (**`Save`**), reject the settings and exit to the CLI (**`Cancel`**), or return to the beginning of the current section and change the settings (**`Retry`**). Entering **`Retry`** displays your previous responses for each prompt. Press **`Return`** to accept the displayed value or enter a new one.

```
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):
```

Configuring the file system

Procedure

1. Enter **`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]:

   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            gz
   Marker type                       auto

   Do you want to save these settings (Save|Cancel|Retry):
   ```

Configuring system parameters

Procedure

1. Enter **`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:
   ddbeta7
   ```

3. Enter 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:
jsmith@yourcompany.com
```

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:
bldg4-rack10
```

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]:
mail.yourcompany.com
```

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, see 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.

Note

Adjusting the time on a DD system is outside of the scope of the wizard. If you need to adjust the time, do so before configuring the NTP service.

```
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 more information about MTrees, see the *EMC Data Domain Operating System Administration Guide*.

1. Enter **yes** to configure the CIFS protocol.

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

2. 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 more information about MTrees, see the *EMC Data Domain Operating System Administration Guide*.

1. Enter **yes** to configure the NFS protocol.

   ```
   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, enter **0** 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*.

Note

Secure Multitenancy (SMT) configuration is an advanced topic; for more information, see the *EMC Data Domain Operating System Administration Guide*.

Rebooting a Data Domain system

The CLI Configuration Wizard will prompt you to reboot your system, 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. Enter **`yes`** to reboot the system.

   ```
   # 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.
   ```

CHAPTER 3

Data Domain System Manager Configuration Wizard

- Getting started with the DD System Manager Configuration Wizard........................24
- Using the DD System Manager Configuration Wizard.. 25

Getting started with the DD System Manager Configuration Wizard

The Data Domain System Manager (DD System Manager) Configuration Wizard is a GUI-based wizard that you can use any time after your initial configuration using either the long or the short form of the CLI Configuration Wizard.

Procedure

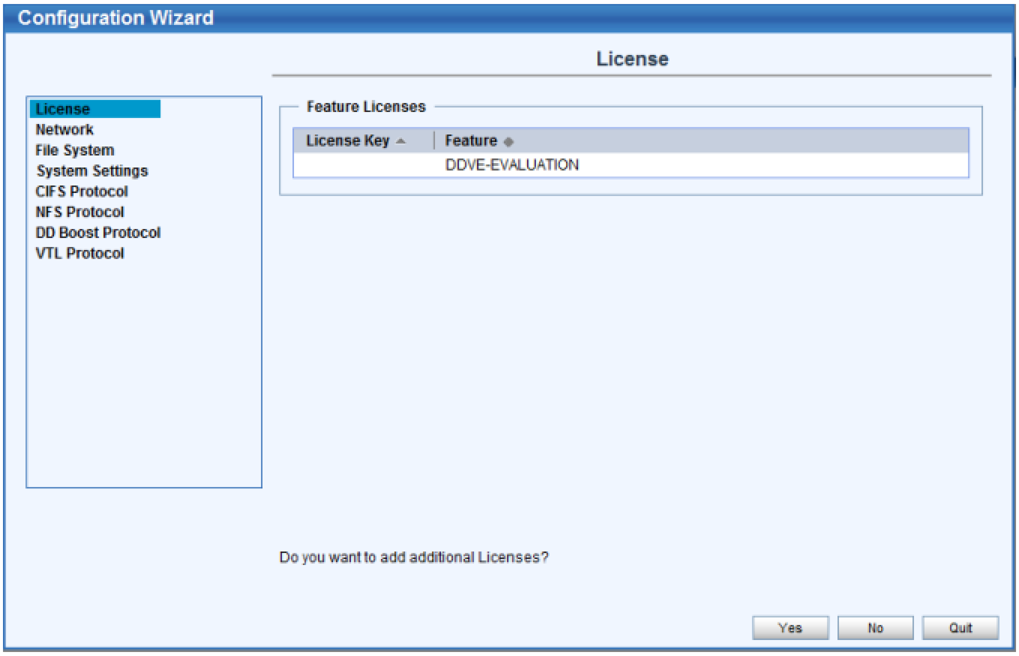
1. If this is the first time you have accessed DD System Manager, open a web browser, and enter your Data Domain system's IP address in the browser's address text box. (If you have previously done this, go to step 3.)
2. When you see the login screen, enter your user name and password, and select **Login**.

   Note

   If you enter an incorrect password 4 consecutive times, the system locks out the specified username for 120 seconds. The login count and lockout period are configurable and might be different on your system. See the *EMC Data Domain Operating System Administration Guide* and the *EMC Data Domain Operating System Command Reference Guide* for how to set these values.

3. Select the DD system that you want to configure from the list of systems on the left.
4. Select **Maintenance** › **System** › **More Tasks** › **Launch Configuration Wizard**.
5. In the Configuration Wizard dialog, the configuration modules are listed on the left. When one of the modules is selected, details are shown on the right. You can configure, or not configure, any module. However, you must start at the first module *License* and either configure or skip every module in order, ending with *VTL Protocol*

Figure 1 DD System Manager Configuration Wizard



License Key	Feature
	DDVE-EVALUATION

Do you want to add additional Licenses?

6. You can now go through the modules using the **Yes**, **No**, **Next**, and **Back** buttons.

Using the DD System Manager Configuration Wizard

The DD System Manager Configuration Wizard lets you configure Licenses, the Network, the File System, System Settings, and the CIFS, NFS, DD Boost and VTL Protocols by going through a series of pages. At any time, you can use the **Quit** button to exit the wizard. For *help* on any page, select the question mark.

Procedure

1. **License**: If you want to add a license, in the Add License Key dialog, enter a single license per line, and press Enter after each one. Select **Add** when you are done.
2. **Network**: Enter as follows:
   a. **General**: Either use a DHCP (Dynamic Host Control Protocol) server to automatically provide these settings, or manually enter the host name, domain name, and gateway IP address.

   b. **Interfaces**: Either use a DHCP server to automatically configure the interfaces, or manually provide the IP addresses and netmasks for each interface. If an interface is disabled, its settings cannot be changed.

   c. **DNS**: Either use a DHCP server to automatically obtain IP addresses for DNS (Domain Name System) servers, or manually add or delete IP addresses.
3. **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. Select one or more available storage IDs and choose **Retention** as the tier configuration. Select the **Add to Tier** button, and select **Next.**

   c. Select the size of the first Retention Unit.

   d. Select **Enable the file system after creation**.
4. **System Settings**: Set up the following to ensure that autosupport (ASUPs) and alert emails from your system are sent to EMC Data Domain.

   a. **Administrator**: Enter a password and email address for the Administrator. Check or uncheck the items that the administrator is to receive at this address.

   b. **Email/Location**: Enter the mail server used to send outgoing alert and ASUPs 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. Verify that the **Send Alert Notification Emails to Data Domain** is selected. Verify that the **Send Vendor Support Notification Emails to Data Domain** is selected. The **Location** field is simply for your information, only.

Note

You currently cannot set up connectEMC using the Data Domain System Manager Configuration Wizard.

c. **Summary**: Review the summary carefully. The default address for alerts and autosupport emails is `autosupport-alert@autosupport.datadomain.com`. The Vendor email is listed as Sending. The vendor email address, which cannot be changed, is `onalert@emc.com`. A detailed autosupport is scheduled to run “daily” at “0600” and is sent to dd_proserv@emc.com, 192.168.10.212 ==> onalert@emc.com. An alert summary is scheduled to run “daily” at “0800” and is sent to dd_proserv@emc.com, 192.168.10.212 ==> onalert@emc.com.

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

   a. **Authentication**: Workgroup: Enter the CIFS server name, if not using the default. Active Directory: Enter the full Realm Name for the system and a Domain Joining Credential user name and password. Optionally, enter the Organizational Unit name, if not using the default.

   b. **Share**: Enter the share name and directory path. Enter the client name, if not using the default.

   c. **Summary**: Review the summary carefully.

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

   a. **Export**: Enter a pathname for the export. Enter the 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.

   b. **Summary**: Review the summary carefully.

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

   a. **Storage Unit**: Optionally, change the Storage Unit name. 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.

   b. **Fibre Channel**: If DD Boost is to be supported over Fibre Channel (FC), select the option to configure it. Enter a unique name for the Access Group. (Duplicate access groups are not supported.) Select one or more initiators. Optionally, replace the initiator by entering a new one. The devices to be used are listed.

   c. **Summary**: Review the summary carefully.

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

   a. **Library**: Enter the library name, number of drives, drive model, number of slots and CAPs, changer model name, starting barcode, and, optionally, tape capacity.

   b. **Access Group**: Enter a unique name for the Access Group. (Duplicate access groups are not supported.) Select one or more initiators. Optionally, replace the initiator name by entering a new one. The devices (drives and changer) to be used are listed.

   c. **Summary**: Review the summary carefully.

9. After completing the wizard:

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

      - If it is not already selected, select the Data Domain system to be rebooted.
      - Select **Maintenance** › **System** › **More Tasks** › **Reboot System**.
      - Select **OK** at the Reboot System confirmation dialog.

   b. Complete the post-configuration tasks in Post-Configuration Setup on page 29.

CHAPTER 4

Post-Configuration Setup

After the initial configuration, perform these post-configuration tasks, as appropriate for your installation.

- Verifying network connectivity 30
- Setting up, testing, and getting autosupports 30
- Setting up ConnectEMC 31
- Configuring security and firewalls (NFS and CIFS access) 32

Verifying network connectivity

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

Procedure

1. From a system with an ssh client network accessible to the DD systems, type:

   ```
   # ssh sysadmin@hostname
   ```

2. From the DD OS CLI, ping the default gateway by typing:

   ```
   # 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.

Setting up ConnectEMC

ConnectEMC is a secure alternative to sending alert and ASUP information in text form.

Procedure

1. To set up the administrator email, enter:

   ```
   # config set admin-email dd_admin1@emc.com
   The Admin Email is: dd_admin1@emc.com
   ```

2. To set the ESRS-gateway (EMC Secure Remote Support), enter:

   ```
   # support connectemc config set esrs-gateway 111.111.11.111
   transport ftp
   ConnectEMC configuration set to "gateway" with transport "ftp".
   ```

3. To add an alternate direct transport email, enter:

   ```
   # support connectemc config add alternate direct transport email
   Added a ConnectEMC alternate: "direct" with transport "email".
   ```

4. To set notification, enter:

   ```
   # support connectemc config set notify-admin always
   Admin will be notified of connectemc events
   ```

5. To enable the sending of autosupports, enter:

   ```
   # support notification enable all
   Enabled sending autosupport and alerts to EMC.
   ```

6. To test that ConnectEMC is enabled, enter:

   ```
   # support connectemc test
   ConnectEMC is enabled. Disable before testing.
   ```

7. To set the notification method to ConnectEMC, enter:

   ```
   # support notification method set connectemc
   Support notification method set to "connectemc".
   ```

8. To show the notification setup, enter:

   ```
   # support notification show all
   Notification   Status    Destination
   ------------   -------   -----------------------
   alerts         enabled   ftp://111.111.11.111:11
   autosupport    enabled   ftp://111.111.11.111:11
   ------------   -------   -----------------------
   ```

9. To show the notification setup, enter:

   ```
   # support connectemc config show
   Notification:   dd_admin1@emc.com  {onSuccess/onFailure}
   Primary:
   ```

```
        Type:          ESRS
        Transport:     FTP
        Destination:   111.111.11.111:11
Alternates:
        Type     Transport   Destination
        ------   ---------   ------------------
        Direct   Email       emailalert@emc.com
        ------   ---------   ------------------
```

10. To disable ConnectEMC to test the configuration after enablement, enter:

```
# support notification method set email
Support notification method set to "email".

# support connectemc test
Sending a test event...
```

11. To re-enable ConnectEMC, enter:

```
# support notification method set connectemc
Support notification method set to "connectemc".
```

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.

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
```

The following tables show the TCP and UDP ports used by the Data Domain system for inbound and outbound traffic, and what service makes use of them.

Table 4 Ports used by Data Domain systems for inbound traffic

Port	Service	Note
TCP 21	FTP	Used only if FTP is enabled (run `adminaccess show` on Data Domain system to determine).
TCP 22	SSH	Used only if SSH is enabled (run `adminaccess show` on Data Domain system to determine).
TCP 23	Telnet	Used only if Telnet is enabled (run `adminaccess show` on Data Domain system to determine).
TCP 80	HTTP	Used only if HTTP is enabled (run `adminaccess show` on Data Domain system to determine).
TCP 111	DDBOOST/ NFS (portmapper)	Used to assign a random port for the mountd service used by NFS and DD Boost. Mountd service port can be statically assigned.
UDP 111	DDBOOST/ NFS (portmapper)	Used to assign a random port for the mountd service used by NFS and DD Boost. Mountd service port can be statically assigned.
UPD 123	NTP	Used only if NTP is enabled (run `ntp status` on Data Domain system to determine).

Table 4 Ports used by Data Domain systems for inbound traffic (continued)

Port	Service	Note
UDP 137	CIFS (NetBIOS name service)	Used by CIFS for NetBIOS name resolution.
UPD 138	CIFS (NetBIOS datagram service)	Used by CIFS for NetBIOS datagram service.
TCP 139	CIFS (NetBIOS session service)	Used by CIFS for session information.
UDP 161	SNMP (query)	Used only if SNMP is enabled (run `snmp status` on Data Domain system to determine).
TCP 389	LDAP	LDAP server listens on this port for any LDAP client request; by default it uses TCP.
TCP 443	HTTPS	Used only if HTTPS is enabled (run `adminaccess show` on Data Domain system to determine).
TCP 445	CIFS (Microsoft-DS)	Main port used by CIFS for data transfer.
TCP 464	Active Directory	“Kerberos change/set password” – required to join an Active Directory domain.
TCP 2049	DD Boost/NFS	Main port used by NFS – can be modified using the `nfs set server-por`t, which requires SE mode.
TCP 2051	Replication/DD Boost/Optimized Duplication	Used only if replication is configured (run `replication show config` on Data Domain system to determine).This port can be modified using `replication modify`.
TCP 2052	NFS Mountd/DD Boost/Optimized Duplication	Main port used by NFS MOUNTD.
TCP 3008	RSS	Required when Data Domain system has an Archive Tier.
TCP 3009	SMS (system management)	Used for managing a system remotely using Data Domain System Manager. This port cannot be modified. This port is used only on Data Domain systems running DD OS 4.7.x or later. This port will also need to be opened if you plan to configure replication from within the Data Domain System Manager, as the replication partner needs to be added to the Data Domain System Manager.
TCP 5001	iPerf	Used, by default, by iPerf. To change the port requires the `-p` option from `se iperf` or the `port` option from `net iperf`. The remote side must listen on the new port.

Table 5 Ports used by Data Domain systems for outbound traffic

Port	Service	Note
TCP 20	FTP	Used only if FTP is enabled (run `adminaccess show` on Data Domain system to determine).
TCP 25	SMTP	Used only if FTP is enabled (run `adminaccess show` on Data Domain system to determine).
UDP/TCP 53	DNS	Used to perform DNS lookups when DNS is configured (run `net show dns` on Data Domain system to review DNS configuration).
TCP 80	HTTP	Used to upload log files to EMC Data Domain support using `support upload`.
TCP 443	HTTPS	Used to upload the Support Bundle (SUB).
UDP 123	NTP	Used to synchronize to a time server.
UDP 162	SNMP (trap)	Used to send SNMP traps to an SNMP host. Use to see destination hosts and `snmp status` to display service status. `snmp show trap-hosts`
UDP 514	Syslog	Used to send syslog messages, if enabled. Use `log host show` to display destination hosts and service status.
TCP 2051	Replication/DD Boost/Optimized Duplication	Used only if replication is configured (run `replication show config` on Data Domain system to determine).
TCP 3009	SMS (system management)	Used for managing a system remotely using Data Domain System Manager. This port cannot be modified. This port is used only on Data Domain systems running DD OS 4.7.x or later. This port will also need to be opened if you plan to configure replication from within the Data Domain System Manager, as the replication partner needs to be added to the Data Domain System Manager.
TCP 5001	iPerf	Used, by default, by iPerf. To change the port requires the `-p` option from `se iperf` or the `port` option from `net iperf`. The remote side must listen on the new port.
TCP 27000	Avamar client communications with Avamar server	Avamar client network hosts.
TCP 27000	Avamar server communications with Replicator target server (Avamar proprietary communication)	Required if server is used as replication source.
TCP 28001	Avamar client communications	Avamar clients required.

Table 5 Ports used by Data Domain systems for outbound traffic (continued)

Port	Service	Note
	with administrator server	
TCP 28002	Administrator server communications with Avamar client	Optional for browsing clients and cancelling backups from Avamar Administrator management console.
TCP 29000	Avamar client Secure Sockets Layer (SSL) communications with Avamar server	Avamar clients required.
TCP 29000	Avamar server SSL communications with Replicator target server	Required if server is replication source.

CHAPTER 5

Additional Configuration Procedures

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

- Changing the timeout on CIFS backup servers 38
- Advanced network configuration 38
- Configuring SNMP on a Data Domain system 43
- Configuring SOL for IPMI 45
- Configuring Encryption for Data at Rest 45
- Optional configuration procedures 45

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 Data Domain Operating System Administration Guide* and the *EMC Data Domain Operating 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 Data Domain Operating System Administration Guide* and the *EMC Data Domain Operating 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 Data Domain Operating System Administration Guide* and the *EMC Data Domain Operating 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.

Procedure

1. To create a virtual interface, enter:

   ```
   # 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. To configure the virtual interface, enter:

   ```
   # 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.

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 modifyvirtual-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 that the associated interfaces on the switch be grouped into an Ethernet truck and 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.

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

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 6

Adding Expansion Shelves

- Adding an expansion shelf.. 48
- Adding enclosure disks to the volume.. 48
- Making disks labeled unknown usable to the system.......................... 49
- Verifying shelf installation..49

Adding an expansion shelf

To install a new expansion shelf, see the *EMC 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 *EMC 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.

Do not mix enclosure and disk types on the same SAS chain.

NOTICE

- Do not remove or disconnect a shelf that has been added earlier. If a shelf is disconnected, the file system volume is immediately disabled and all data in the volume is lost.
- To re-enable a shelf, reconnect the shelf or transfer the disks from the shelf to another empty shelf chassis and connect.
- if the data on a shelf is not available to the file system volume, the volume cannot be recovered.
- Unless the same disks are available to the file system, the DD OS must be re-installed as directed by your contracted service provider or the EMC Online Support site, http://support.emc.com.

Adding enclosure disks to the volume

Procedure

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

   ```
   # storage add enclosure enclosure-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. Because the disks cannot be removed from the file system without re-installing the DD OS after they have been added, you are asked to confirm. Enter:

   ```
   y
   ```

3. When prompted, enter your sysadmin password.
4. (optional) Add disks in another enclosure at this time, by entering:

   ```
   # storage add enclosure enclosure-id
   ```

5. Display the RAID groups for each shelf by entering:

   ```
   # storage show all
   ```

   For the ES30, one disk in a shelf is a spare disk. The rest should report that they are available.

6. To allow the file system to use these enclosure disks, enter:

   ```
   # filesys expand
   ```

Making disks labeled unknown usable to the system

Making disks labeled unknown usable to the system 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

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

Procedure

1. Check the status of the SAS HBA cards:

   ```
   # disk port show summary
   Port   Connection   Link     Connected       Status
          Type         Speed    Enclosure IDs
   ----   -----------  ------   -------------   ------
   2a     SAS          12 Gbps  4               online
   2b     SAS                                   offline
   2c     SAS                                   offline
   2d     SAS                                   offline
   3a     SAS          24 Gbps  2               online
   3b     SAS                                   offline
   3c     SAS                                   offline
   3d     SAS                                   offline
   6a     SAS          12 Gbps  4               online
   6b     SAS                                   offline
   6c     SAS          24 Gbps  3               online
   6d     SAS                                   offline
   9a     SAS                                   offline
   9b     SAS                                   offline
   9c     SAS                                   offline
   9d     SAS          24 Gbps  2               online
   ```

   The output shows:

   - The `online` status for each SAS connection, such as `2a`, `3a`, `6a` .

- The `offline` status for each SAS connection, such as `2b`, `3b`, `6b`.
- After the shelves have been connected, the same command also displays the connected enclosure IDs for each port. The status changes to `online`.

2. Verify the disk state:

```
# disk show state
Enclosure Disk
           1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
--------- ----------------------------------------------
1          .  .  .  .
2          U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3          s  U  U  U  U  U  U  U  U  U  U  U  U  U  F
4          U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
5          A  K  v  K  K  K  K  K  K  v  K  K  K  K  R
--------- ----------------------------------------------

Legend   State                          Count
------   ----------------------------   -----
.        In Use Disks                   4
s        Spare Disks                    1
R        Spare (reconstructing) Disks   1
v        Available Disks                2
K        Known Disks                    11
U        Unknown Disks                  43
F        Failed Disks                   1
A        Absent Disks                   1
------   ----------------------------   -----
Total 64 disks
```

Note

All added disks are in `U` state.

3. Verify that the Data Domain system recognizes each attached enclosure/shelf:

```
# enclosure show summary
Enclosure Model No. Serial No.     State  OEM  OEM   Capacity
                                          Name Value
--------  --------- -------------- ------ ---- ----- --------
1         DD9500    NVT10133200020 Online             4 Slots
2         ES30      APM00133825711 Online            15 Slots
3         ES30      APM00120900626 Online            15 Slots
4         ES30      APM00123706119 Online            15 Slots
5         ES30      APM00133825239 Online            15 Slots
--------  --------- -------------- ------ ---- ----- --------
5 enclosures present.
```

The output shows each recognized enclosure ID, Data Domain system model number, serial number, and slot capacity.

4. Verify that the system is in good running condition and shows no errors:

```
# enclosure show topology
Port     enc.ctrl.port     enc.ctrl.port     enc.ctrl.port
----  -  -------------  -  -------------  -  -------------
2a
2b    >  2.B.H: 2.B.E   >  3.B.H: 3.B.E   >  4.B.H: 4.B.E
2c    >  5.B.H: 5.B.E
2d
3a    >  5.A.H: 5.A.E
3b
3c    >  4.A.H: 4.A.E   >  3.A.H: 3.A.E   >  2.A.H: 2.A.E
3d
----  -  -------------  -  -------------  -  -------------
Encl   WWN                Serial #
----   ----------------   --------------
2      N/A                APM00134300550
```

```
3      N/A                APM00134300549
4      N/A                APM00134300556
5      N/A                APM00134300555
----   ----------------   --------------
Error Message:
-----------------
No error detected
-----------------
ES20 rear view:
                 CONTROLLER-B   CONTROLLER-A   OP-PANEL
+--------------------------------------------------------+
|                |     E      |      H      |            |
|                |            |             |            |
|                |     H      |      E      |            |
+--------------------------------------------------------+
ES30 rear view:
+--------------------------------------------------------+
CONTROLLER-B     |           E             H             |
+--------------------------------------------------------+
+--------------------------------------------------------+
CONTROLLER-A     |           H             E             |
+--------------------------------------------------------+
```

APPENDIX A

Time Zones

This appendix covers the following topics:

- Time zones overview ... 54
- Africa ... 54
- America ... 54
- Antarctica ... 56
- Asia ... 56
- Atlantic ... 57
- Australia ... 57
- Brazil ... 57
- Canada ... 57
- Chile ... 58
- Etc ... 58
- Europe ... 58
- GMT ... 59
- Indian (Indian Ocean) ... 59
- Mexico ... 59
- Miscellaneous ... 59
- Pacific ... 60
- US (United States) ... 60
- Aliases ... 60

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

Table 6 African time zones

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

Table 7 American time zones

Adak	Anchorage	Anguilla	Antigua	Araguaina

Table 7 American time zones (continued)

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

Table 7 American time zones (continued)

St_Vincent	Swift_Current	Tegucigalpa	Thule	Thunder_Bay
Tijuana	Toronto	Tortola	Vancouver	Virgin
Whitehorse	Winnipeg	Yakutat	Yellowknife	

Antarctica

Table 8 Antarctic time zones

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

Asia

Table 9 Asian time zones

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

Table 9 Asian time zones (continued)

Vladivostok	Yakutsk	Yekaterinburg	Yerevan	

Atlantic

Table 10 Atlantic time zones

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

Australia

Table 11 Australian time zones

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

Table 12 Brazilian time zones

Acre	DeNoronha	East	West

Canada

Table 13 Canadian time zones

Atlantic	Central	East-Saskatchewan	Eastern
Mountain	Newfoundland	Pacific	Saskatchewan
Yukon			

Chile

Table 14 Chilean time zone

Continental	EasterIsland

Etc

Table 15 Etc time zones

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

Table 16 European time zones

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

Table 17 GMT time zones

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)

Table 18 Indian (Indian Ocean) time zones

Antananarivo	Chagos	Christmas	Cocos	Comoro
Kerguelen	Mahe	Maldives	Mauritius	Mayotte
Reunion				

Mexico

Table 19 Mexican time zones

BajaNorte	BajaSur	General

Miscellaneous

Table 20 Miscellaneous time zones

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

Table 20 Miscellaneous time zones (continued)

Turkey	UCT	Universal	UTC	WET
W-SU	Zulu			

Pacific

Table 21 Pacific time zones

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)

Table 22 US (United States) time zones

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