## Contents

**About This Guide** ......................................................... 7  
  Related Documents ..................................................... 7  
    Access to Integration-Related Documents at Data Domain  8  
      Access Data Domain Documents ................................. 8  
  Conventions .................................................................. 9  
  Audience ....................................................................... 10  
  Contacting Data Domain ............................................... 10  

1 **Getting Started** ....................................................... 11  
  Installation and Configuration Overview ......................... 11  
    Prerequisites .................................................................. 12  
    Obtain this Information Before You Start .................... 13  
      About Licenses .......................................................... 15  
  Initial System Setup ....................................................... 16  
    Set Up a DD690g or DD880g System .............................. 16  
    Set Up a DD460g, DD560g, or D580g System .................. 17  
    Set Up a Data Domain System Using the CLI ................. 18  

2 **The Configuration Wizard** ........................................... 19  
  Working with the CLI Configuration Wizard ..................... 20  
  Licenses ......................................................................... 21  
  Network .......................................................................... 21  
  Configure the Network .................................................. 21
Additional Physical or Virtual Interface Configuration . . 43
  Specify the MTU ........................................ 43
  Configure Duplex Line Use and Speed .................. 44
  Set Auto-negotiate for an Interface .................... 45
Routing Tables and Gateways ............................. 45
Configuring SNMP on a Data Domain System ............. 45
  Add a Community String ................................ 45
  Enable SNMP ........................................... 46
  Set the System Location ............................... 46
  Set a System Contact ................................ 46
  Add a Trap Host ....................................... 47
Configuring SOL for IPMI ................................. 47
Configuring Encryption of Data at Rest .................. 48
Optional Configuration Procedures ....................... 48
4 Adding Expansion Shelves and Third-Party LUNs . . . 51
  Adding Expansion Shelves .............................. 51
  Verify Shelf Installation ............................... 52
  Add Enclosure Disks to the Volume .................... 52
  Disks Labeled Unknown Instead of Spare ............... 53
  Adding a Third-Party LUN to a Gateway Systems ........ 53
  Create and Verify the New LUN ....................... 53
  Add the LUN to the Data Domain File System .......... 54
A Time Zones ............................................ 55
  Africa ............................................... 56
  America ............................................. 56
<table>
<thead>
<tr>
<th>Location</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antarctica</td>
<td>57</td>
</tr>
<tr>
<td>Asia</td>
<td>57</td>
</tr>
<tr>
<td>Atlantic</td>
<td>58</td>
</tr>
<tr>
<td>Australia</td>
<td>58</td>
</tr>
<tr>
<td>Brazil</td>
<td>58</td>
</tr>
<tr>
<td>Canada</td>
<td>58</td>
</tr>
<tr>
<td>Chile</td>
<td>59</td>
</tr>
<tr>
<td>Etc</td>
<td>59</td>
</tr>
<tr>
<td>Europe</td>
<td>59</td>
</tr>
<tr>
<td>GMT</td>
<td>60</td>
</tr>
<tr>
<td>Indian (Indian Ocean)</td>
<td>60</td>
</tr>
<tr>
<td>Mexico</td>
<td>60</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>60</td>
</tr>
<tr>
<td>Pacific</td>
<td>61</td>
</tr>
<tr>
<td>System V</td>
<td>61</td>
</tr>
<tr>
<td>US (United States)</td>
<td>61</td>
</tr>
<tr>
<td>Aliases</td>
<td>62</td>
</tr>
</tbody>
</table>
About This Guide

This guide explains how to perform initial configuration of the Data Domain® system.

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

Related Documents

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

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

- Data Domain Operating System Release Notes, Version 5.0.x
- DD OS 5.0 Administration Guide
- DD OS 5.0 Command Quick Reference
- DD OS 5.0 Command Reference Guide
- Data Domain Hardware Guide
- Data Domain Expansion Shelf Hardware Guide
- Data Domain Boost for OpenStorage Administration Guide
- DD860 Archiver Administration Guide
- The Data Domain system installation and setup guides for each of the supported platforms (for example DD880, DD690g, and so forth).
Access to Integration-Related Documents at Data Domain

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

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

Access Data Domain Documents

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

c. Select the desired title from the list and click View.

4. To view compatibility matrices, perform the following steps:

a. Click Compatibility Matrices.

b. Select the desired title from the product menu and click View.

## Conventions

The following tables describe the typographical conventions used in this guide.

<table>
<thead>
<tr>
<th>Typeface or Symbol</th>
<th>Usage</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monospace</td>
<td>Commands, command options, and parameters and computer output.</td>
<td>Use the <code>config</code> command to manage the Data Domain system configuration settings.</td>
</tr>
<tr>
<td><strong>Monospace bold</strong></td>
<td>Commands the user types at the command prompt (#).</td>
<td>Enter: <code># config setup</code></td>
</tr>
<tr>
<td><strong>Monospace italic bold</strong></td>
<td>Command variables the user types at the command prompt (#).</td>
<td><code># log view file_name</code></td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>Book titles, and variables.</td>
<td>Refer to the <em>DD OS 5.0 Command Reference Guide</em> for complete descriptions of DD OS commands.</td>
</tr>
<tr>
<td>Pipe (</td>
<td>) and curly braces ({{})</td>
<td>Choose (pipe) between a required argument (curly braces) in the CLI.</td>
</tr>
<tr>
<td>Brackets ([[]) and ellipses (...))</td>
<td>One or more (list with commas and ellipses) optional (bracket) arguments in the CLI.</td>
<td><code>[arg1, arg2, ...]</code></td>
</tr>
</tbody>
</table>
Audience

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

Contacting Data Domain

To resolve issues with Data Domain products, contact your contracted support provider or visit us online at https://my.datadomain.com.
1 Getting Started

The Data Domain Operating System (DD OS) is pre-installed on a Data Domain system. You need to configure the DD OS using the Data Domain Configuration Wizard, which is available through the command-line-interface (CLI).

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

This chapter covers the following topics
- Installation and Configuration Overview on page 11
- Initial System Setup on page 16

Installation and Configuration Overview

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

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

2. Define the Data Domain system information for your site as described in Prerequisites on page 12.

3. Perform the initial software configuration, at the console, using the command line interface (CLI). See The Configuration Wizard on page 19.

4. Reboot the Data Domain system.
5. Test the network connections.

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

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

8. If using VTL, configure backup software for VTL data access and then set up the Data Domain system to use VTL (see the *DD OS 5.0 Administration Guide*).

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

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

**Prerequisites**

This guide assumes the following tasks have been completed:

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

2. If the system is a Data Domain Gateway system:
   a. The third-party external storage has been installed.
   b. The logical units (LUNs) for use by the Data Domain system have been created, and LUN masking and SAN zoning have been configured. See the Integration Documentation and Compatibility Matrices for the relevant third-party applications.

3. An administrative console has been set up to communicate with the system as described in the *Data Domain Installation and Setup Guide*. You can use either a serial console or a monitor and keyboard.
Obtain this Information Before You Start

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

2. Have the information described in Table 1-1 available for you to enter during the configuration procedure.

Table 1-1: Information to Enter During Configuration

<table>
<thead>
<tr>
<th>Required</th>
<th>Description</th>
<th>Your Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login default password</td>
<td>This value is the Data Domain system’s serial number, located on its rear panel.</td>
<td></td>
</tr>
<tr>
<td>Licenses</td>
<td>A license consists of characters in this format: ABCD-ABCD-ABCD-ABCD. For more information, see About Licenses on page 15.</td>
<td></td>
</tr>
<tr>
<td>If using the Dynamic Host Configuration Protocol (DHCP), obtain the MAC address of the network port.</td>
<td>The Media Access Control (MAC) address consists of 12 alphanumeric characters which are printed on a label under each Network Interface Card (NIC), located below the Ethernet port. This information is used to configure your DHCP server, which will assign an IP address for the Data Domain system.</td>
<td></td>
</tr>
</tbody>
</table>
3. If you are not using DHCP, determine the values listed in Table 1-2, which you need to enter during the configuration procedure.

**Table 1-2:** Network Configuration Values (Non-DHCP)

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

4. If using a Gateway or Virtual Tape Library, obtain the WWN numbers.

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

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

Licenses are required for these installed features:

- **Data Domain OpenStorage (DD Boost) software.**
  
  Enables the use of a Data Domain system with Symantec Veritas NetBackup (NBU) OpenStorage (OST).

  **Note:** The optimized duplication feature of DD Boost also requires the Replication license.

- **Expansion Storage License**
  
  Allows the upgrade of capacity for the Data Domain system. Enables either the upgrade of a 9-disk DD510/DD530 to 15 disks, or the upgrade of a 7-disk DD610/DD630 to 12 disks.

- **Gateway Expanded Storage Level 2**
  
  Enables gateway systems to support up to 71 TB of usable capacity.

- **Gateway Expanded Storage Level 3**
  
  Enables gateway systems to support up to 145 TB of usable capacity.

- **VTL**
  
  Enables the use of a Data Domain system as a virtual tape library.

- **Replication**
  
  Uses the Data Domain Replicator to replicate data from one Data Domain system to another. A license is required on each system.

- **Retention Lock**
  
  This license covers two features:

  - **Retention Lock** protects selected files from modification and premature deletion, that is, deletion before a specified retention period has expired.
- *System sanitization* ensures that all traces of deleted files are completely disposed of and that the system is restored to a state as if the deleted files never existed.

- Encryption of Data at Rest
  Allows data on system drives or external storage to be encrypted while being saved, and then locked before moving to another location. This protects data from being viewed by unauthorized persons should any device become lost or stolen during transit. The device is then unlocked at the destination.

- Nearline
  Identifies systems that are deployed for archive and nearline workloads.

- Global Deduplication
  Licenses the global deduplication feature.

- DD860 Archiver
  Licenses the archive storage feature. See the *DD860 Archiver Administration Guide* for additional information.

## Initial System Setup

*Note:* The setup procedure depends on whether you are logging into a Data Domain system that includes storage, such as the DD690, or logging into a gateway system. A gateway system, such as the DD690g, stores all data on third-party storage using a fiber channel connection.

### Set Up a DD690g or DD880g System

1. Verify that the system is powered on.
2. When prompted, enter `sysadmin` as your login name.
3. Enter the default password (the Data Domain system’s serial number).
4. Enter:
   
   # disk rescan
5. Find out the name of the device by entering:

   # storage show all

6. To enable the Data Domain system to recognize the device, enter:

   # storage add devx

   where devx is the name of the device, such as dev3.

7. After the storage add command completes, verify that the file system is up and running, by entering:

   # filesys status

You can attach a VGA monitor and log in using the CLI to configure the system, as described in the section Set Up a Data Domain System Using the CLI on page 18.

Set Up a DD460g, DD560g, or D580g System

1. Verify that the system is powered on.

2. During the initial system start, the Data Domain system does not know about available Logical Unit Numbers (LUNs).

   The New Install menu is displayed with the first menu item, Do a New Install, selected:

   New Install
   1. Do a New Install
   2. Show Configuration
   3. Reboot

3. Press the down-arrow key to select the second menu item, Show Configuration, and press Enter.

4. The System Configuration (Before Installation) menu is displayed. The first item—Show Storage Information—is selected. Press Enter to display the storage information.

   In the output that is displayed:

   • Each LUN that is available from the array system appears as a one-line entry in the List of SCSI Disks/LUNs.
Note: If the LUNs do not show, check the configuration of the storage management/SAN zoning.

- The Valid RAID Disk Group UUID List section does not show any disk groups until after installation.

5. Use the arrow keys to move up and down in the display.

6. Press Enter to return to the New Install menu.

7. Use the up-arrow key to select the first menu item, Do a New Install.

8. Press Enter to start the installation. The system automatically configures all LUNs available from the array.

9. Press Enter again to confirm the new installation. No other user input is required.

10. When the reboot completes, the login prompt is displayed.

After the Data Domain system verifies the external storage arrays, you can attach a VGA monitor and log in using the CLI to configure the system via the Enterprise Manager.

Set Up a Data Domain System Using the CLI

Log in using a serial console or a VGA monitor and keyboard.

1. At the login prompt, enter sysadmin

2. When prompted for the password, enter the Data Domain system’s serial number.

3. When prompted to change the password, enter y and type a new password.

   The Configuration Wizard starts automatically. Until the configuration is complete, the Configuration Wizard command reappears whenever you log in.

4. Follow the appropriate instructions given in The Configuration Wizard on page 19.
2 The Configuration Wizard

The Configuration Wizard consists of these sections: Licenses, Network, Filesystem, System, CIFS, and NFS. You can configure or skip any section. After completing the Configuration Wizard, reboot the Data Domain system.

Notes:

- The Configuration Wizard performs an “initial” configuration—it does not cover all configuration options, it only configures what is needed for the most basic system setup. After initial configuration, you can use the Enterprise Manager or individual CLI commands to change or update the configuration.

- If you have already configured your system as described in the *Data Domain Installation and Setup Guide*, you can refer to this chapter for more detailed information when you need to reconfigure your system.

- The Filesystem configuration is not described here, as the default values are acceptable to most sites. If you wish to configure these settings, see the `filesys` command and options for setting local and global compression and marker types.

- When configuring a Data Domain system as part of a Replicator pair, follow the same configuration steps as for a single system.

This chapter covers the following topics:

- Working with the CLI Configuration Wizard on page 20
- Licenses on page 21
- Network on page 21
- System on page 22
Working with the CLI Configuration Wizard

If the CLI Configuration Wizard does not start immediately the first time you log in, you can run it at any time by entering the command:

```
# config setup
```

For each configuration section, you are prompted to answer a series of questions. Follow these procedures:

- Type `y` to configure a section.
- Type `n` to skip a section and go to the next one.
- Type a question mark (`?`) at a prompt to display more information.
- 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 the 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 hostname, such as `srvr22.company.com`.

At the end of each section, a summary of your entries is displayed. You can accept or reject your changes and go to the next section, or return to the beginning of that section and change any of the settings. When you select Retry, you are shown your previous entries for each prompt.
To exit the CLI, you have to configure or skip each of the sections, or enter Ctrl+C.

After the configuration is completed, the CLI prompts you to reboot the system if a reboot is required.

**Licenses**

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

If you have not licensed a category, make no entry. If using the CLI, press the Enter key.

**Network**

Working with the network consists of:

- Configure the Network on page 21
- Configure Ethernet Interfaces (Ports) on page 21

**Configure the Network**

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

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

**Configure Ethernet Interfaces (Ports)**

1. Enable the port.

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

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

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

4. If any of the ports are not using DHCP, specify an IP address for a default routing gateway.

5. If none of your network ports is configured to use DHCP, or DHCP is not configured to provide the DNS servers, you can specify one, two, or three DNS servers to resolve hostnames with IP addresses. Do one of the following:
   - Enter the server name or names, separating items in the list with either a comma or a space, or
   - Choose to enter no servers by pressing the Enter key. In this case, use the `net hosts` command, which is described in the *DD OS 5.0 Command Reference Guide*, to inform the Data Domain system of IP addresses for hostnames.

6. Press Enter.

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

After saving the port configuration, allow up to two minutes for the Data Domain system to update the interfaces.

**System**

Enter the following information:

- Admin Host

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

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

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

**Notes:**

- The **autosupport feature** sends a daily report to Data Domain Support that shows system identification information and consolidated output from Data Domain system commands and entries from various log files.

- Alerts occur whenever the system’s Restore Protection Manager discovers a problem with software or a monitored hardware component. The **alert command** manages the alerts history file and who receives email notification for system alerts.

- For more information about autosupport and alerts, see the **DD OS 5.0 Administration Guide**.

- **System Location**
  
  Enter a physical location that identifies this system for use in autosupport emails. For example, enter Bldg4-rack10. The alerts and autosupport reports display the location.

- **SMTP Mail Server**
  
  Enter the name of a local SMTP (mail) server that relays Data Domain system emails. If the server is an Exchange server, be sure that SMTP is enabled.

- **Time Zone**
  
  The system date is already set.
Using the tables in Time Zones on page 55, determine your local time zone. The default time zone for each Data Domain system is US/Pacific.

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

- Network Time Service (NTP) Servers
  The default is to enable NTP and to use multicast for NTP.
  
  If DHCP is set up, do the following only if the DHCP server is not configured to provide the NTP servers:
  
  To allow the Data Domain system to use one or more Network Time Service (NTP) servers to synchronize its clock, enter their IP addresses or server names, separated by commas.

CIFS

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

The /backup directory is the destination directory on the Data Domain system for compressed backup server data.

Create a CIFS Share Using the Enterprise Manager

1. Select one of these authentication methods for access to the /backup directory on the Data Domain system:
   
   - Active-Directory: The full realm name for the system, such as domain1 and domain1.local.
   
   - Workgroup: A CIFS workgroup account that sends backups to the Data Domain system. You can enter a backup user name and password.

2. (Optional) Enter the IP address for the Windows Internet Name Service (WINS) server for this system if you want it to dynamically map IP addresses to computer names.
3. **Backup Server List:** Enter between one and ten backup servers as Data Domain system clients, separated by commas. You can enter fully qualified domain names, hostnames, or IP addresses. A single asterisk (*) as a wild card indicates that all backup servers can be used as clients.

   **Note:** `admin_host` is implicitly part of the Backup Server list.

4. **(Active-Directory)** To join a Domain now, enter a domain controller administrator account name and password.

---

**NFS**

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

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

Using the Enterprise Manager, you can add NFS clients to `/backup`. 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.

---

**Security and Firewalls**

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

Please consult with your Data Domain system engineer 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, change this option from disabled (the default) to enabled:

```
# cifs option set restrict-anonymous enabled
```
Rebooting the Data Domain System

After configuring the system, reboot the Data Domain system using the CLI.

Enter:

```
# system reboot
```

*Note:* If you are using the Enterprise Manager, log out of the Enterprise Manager and close its Web-browser window before entering the `system reboot` command. Otherwise, warning messages might display when the system reboots.

Verifying Network Connections

It is recommended that each Data Domain interface on which traffic is expected is tested for connectivity using the ping command.

Enter:

```
# ping hostname
```

where `hostname` is the hostname or an IP address associated with the interface being tested. Each interface must have a unique hostname or IP address.

About the /ddvar Directory

The `/ddvar` directory contains Data Domain system core and log files. The `/ddvar` directory has the following subdirectories:

- `core`, which is the default destination for core files created by the system.
- `log`, which is the destination for all system log files.
- `releases`, which is the default destination for operating system upgrades that are downloaded from the Data Domain Support Web site.
- `snmp`, which is the location of the SNMP (Simple Network Management Protocol) MIB (Management Information Base).
• **support**, which is where logs and autosupport files, as well as new DD OS images are stored. Access this directory to send autosupport files for Support, and for images for upgrading the Data Domain system. You can enable a CIFS share or NFS export to this location, as well as use FTP.

• **traces**, which is the destination for execution traces used in debugging performance issues.

NFS and CIFS clients that have administrative access need to be able to access this directory. NFS clients can be set up using the Enterprise Manager. CIFS client shares to /ddvar must be set up using the CLI.

### Create a CIFS Share to /ddvar

When only one CIFS client is allowed to access the share, enter:

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

If more than one client is to have access, use the `cifs share create` command.

Enter:

```bash
# cifs share create share-name path path {max-connections number | clients "client-list" | browsing {enabled | disabled} | writeable {enabled | disabled} | users "user-names" | comment "comment"}
```

where:

- **share-name**: a descriptive name for the share.
- **path**: the path to the target directory.
- **number**: the maximum number of connections to the share that are allowed at one time.
- **client-list**: a comma-separated list of clients that are allowed to access the share. No blank or tab (white space) characters are allowed. The list must be enclosed in double quotation marks. For example,

  "host1,host2"

  "host1,10.24.160.116"
• **browsing**: the share can be seen (enabled, which is the default), or not seen (disabled) by web browsers.

• **writeable**: the share can be writable (enabled, the default), or not writable (disabled).

  **Note:** All administrative users have write privileges, by default, even if writable is disabled.

• “**user-names**”: a comma-separated list of user names. Other than the comma delimiter, any white space (blank or tab) characters are treated as part of the user name because a Windows user name can have a space character in the name. The list must be enclosed in double quotation marks. For example: "user1,user2" or "user1,@group1"

  The user names list can include group names, which must be proceeded by the *at* (@) symbol; such as @group1.

  All users in the client list can access the share, unless one or more user names are specified, in which case only the listed names can access the share. Group names and user names should be separated only by commas, not spaces. There can be spaces inside the name of a group, but there should not be spaces between groups.

• **comment**: a descriptive comment about the share.

The following example creates a share that can be accessed by two users:

```
# cifs share create dir2 path /backup/dir2 clients * users "dsmith,jdoe" comment "This share can be accessed only by dsmith and jdoe."
```

### Configuring the Data Domain System for Data Access

After completing the Configuration Wizard, you need to configure the clients that access the Data Domain system.


2. In the Navigation pane, click Documentation.
3. On the Documentation page, click Integration Documentation.
4. Select the vendor for the client system’s operating system, such as Sun or Microsoft, and click OK.
5. Select the appropriate tuning document, such as Solaris System Tuning or the CIFS Tuning Guide.

**Powering Off the Data Domain System**

Power off the Data Domain system for the following:

- part replacement
- system relocation
- a planned power outage

Enter:

```
# system poweroff
```
3  Additional Configuration

This chapter describes some additional configuration procedures that are performed once the initial configuration with the Configuration Wizard is complete. This chapter covers the following major topics:

- Changing the Timeout on CIFS Backup Servers on page 31
- Optional Configuration Procedures on page 48
- Multipath Monitoring on page 32
- Advanced Network Configuration on page 33
- Configuring SNMP on a Data Domain System on page 45
- Configuring SOL for IPMI on page 47
- Configuring Encryption of Data at Rest on page 48
- Optional Configuration Procedures on page 48

Changing the Timeout on CIFS Backup Servers

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

Change the Default Timeout Value

1. Open the Registry Editor on the Windows machine. Go to Start > Run and type this in the Open text box:

   REGEDT32

2. Click OK.
3. Expand the My Computer node in the left pane.

4. Expand HKEY_LOCAL_MACHINE and continue to expand nodes in the directory tree until you reach the parameters menu from this path: SYSTEM > CurrentControlSet > Services > lanmanworkstation > parameters.

5. If there is a SESSTIMEOUT key, it is located in the name list in the right pane. If there is no such key, right-click within an empty space in the right pane, select New > Key, and name the new key SESSTIMEOUT, using all caps.

6. Double-click the SESSTIMEOUT key and set its value to 300.

**Multipath Monitoring**

If your Data Domain system has been physically configured with more than one path, you need to set up monitoring for the multipath feature.

Multipath allows external storage I/O paths to be used for failover across paths. When a Data Domain system has been physically configured with more than one path and it fails, the system fails over, that is, it uses the other path. There is no interruption of service.

After physically setting up external storage I/O paths for failover, the Data Domain system is set to monitor multipathing. When monitoring is enabled (the default), any failures in paths to disk devices trigger alerts and log multipath events.

**Set Up Multipath Monitoring**

*Note:* Multipath monitoring is enabled by default.

1. Verify that the physical port connections have been configured for the Data Domain system by entering:

   ```bash
   # disk port show summary
   ```

   The output depends on the Data Domain mode; for example:

   - For a gateway system, the command output shows port, connection type, link speed, port ID, connected number of LUNs, and status.
• For an ES20 Expansion Shelf, the command output shows port, connection type, link speed, connected enclosure IDs, and status.

2. Enter:

   # disk multipath option set monitor {enabled | disabled}

   **Note:** If you make any multipath configuration changes after monitoring is enabled, reset monitoring using the `disk multipath option reset monitor` command and then enable (set) monitoring.

3. Enter:

   # disk multipath status

   The output shows the configured paths. Verify that multipathing is setup correctly.

### Advanced Network Configuration

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

• **Ethernet Failover**

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

• **Link Aggregation**

  You can combine multiple 1 GbE ports into a virtual interface for link aggregation. With link aggregation, either two or four Ethernet network ports can be used in parallel, which increases the link speed and also provides a reduced performance failover capability over that of a single port.

• **VLAN Tagging**

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

**About the Ethernet Interface Ports**

The Ethernet port naming convention used for all Data Domain systems shipped prior to DD OS 4.9 included only a number for each port without regard to physical location of that port (for example, eth0 to eth5). Starting with new systems shipped with 4.9, the Ethernet Interface naming scheme references both 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).

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

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

**Pre-DD OS 4.9 Port Naming and Port Combinations**

**Note:** For systems deployed before the arrival of DD OS 4.9, the port naming convention is retained when the DD OS is upgraded.

A Data Domain system deployed before DD OS 4.9 can have up to six physical Ethernet interface ports.

**Table 3-1** shows which physical pairs are supported, based on the application. There are no similar restrictions for VLAN configuration.

**Table 3-1:** Supported Ethernet Port Pairs, Pre-DD OS 4.9

<table>
<thead>
<tr>
<th>Link Aggregation or Failover, 1 GbE Ports</th>
<th>Failover, 10 GbE Ports (Dual-port CX4 copper only, no single-port optical&lt;sup&gt;a&lt;/sup&gt;)</th>
<th>Failover, 10GbE Ports (Dual-port SFP+ copper and optical&lt;sup&gt;b&lt;/sup&gt;)</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0 with eth1, eth2, eth3, eth4, or eth5</td>
<td>eth2-eth3</td>
<td>eth2 with eth3, eth4, or eth5</td>
</tr>
</tbody>
</table>

<sup>a</sup> Dual-port CX4 copper (no single-port optical)

<sup>b</sup> Dual-port SFP+ copper and optical
For systems that initially shipped with DD OS 4.9, the slot-based port naming conventions is used, and the following rules apply:

- A Data Domain system can have up to eight physical Ethernet interface ports (eth0a, eth0b, eth1a, eth1b, eth4a, eth4b, eth5a, and eth5b). See your Data Domain system hardware documentation for port locations.

- Limitations for failover and link aggregation for pre-DD OS 4.9 1 GbE ports apply here as well. See Configure Failover on page 39 and Configure Link Aggregation on page 40.

- 10 GbE copper-to-10 GbE copper ports across Intel NICs can be combined for failover (but not for link aggregation).

- 10 GbE optical-to-10 GbE optical ports can be combined for failover (but not for link aggregation). This excludes single-port optical cards.

- 10 GbE failover across Intel NICs is supported (not between copper and optical).

- 10 GbE link aggregation is not supported.

**Table 3-1: Supported Ethernet Port Pairs, Pre-DD OS 4.9**

<table>
<thead>
<tr>
<th>Link Aggregation or Failover, 1 GbE Ports</th>
<th>Failover, 10 GbE Ports (Dual-port CX4 copper only, no single-port optical(^a))</th>
<th>Failover, 10GbE Ports (Dual-port SFP+ copper and optical(^b))</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth1 with eth2, eth3, eth4, or eth5</td>
<td>eth4-eth5</td>
<td>eth3 with eth4 or eth5</td>
</tr>
<tr>
<td>eth2 with eth3, eth4, or eth5</td>
<td></td>
<td>eth4 with eth5</td>
</tr>
<tr>
<td>eth3 with eth4 or eth5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth4 with eth5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\(^a\) Single-port optical NICs cannot be used in failover \\
\(^b\) Failover across copper and optical ports is not supported

**DD OS 4.9 Port Naming and Port Combinations**

For systems that initially shipped with DD OS 4.9, the slot-based port naming conventions is used, and the following rules apply:

- A Data Domain system can have up to eight physical Ethernet interface ports (eth0a, eth0b, eth1a, eth1b, eth4a, eth4b, eth5a, and eth5b). See your Data Domain system hardware documentation for port locations.

- Limitations for failover and link aggregation for pre-DD OS 4.9 1 GbE ports apply here as well. See Configure Failover on page 39 and Configure Link Aggregation on page 40.

- 10 GbE copper-to-10 GbE copper ports across Intel NICs can be combined for failover (but not for link aggregation).

- 10 GbE optical-to-10 GbE optical ports can be combined for failover (but not for link aggregation). This excludes single-port optical cards.

- 10 GbE failover across Intel NICs is supported (not between copper and optical).

- 10 GbE link aggregation is not supported.
Table 3-2 through Table 3-4 show which physical pairs are supported, based on the application and controller model. There are no restrictions for VLAN configuration.

**Table 3-2: Supported Ethernet Port Pairs, DD OS 4.9 on DD880**

<table>
<thead>
<tr>
<th>Link Aggregation or Failover, 1 GbE Ports</th>
<th>Failover, 10 GbE Ports (Dual-port CX4 copper only, no single-port optical)</th>
<th>Failover, 10GbE Ports (Dual-port SFP+ copper and optical)</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0a with eth0b, et4a, eth4b, eth5a, or eth5b</td>
<td>eth5a-eth5b</td>
<td>eth5a with eth5b, eth4a, or eth4b</td>
</tr>
<tr>
<td>eth0b with eth4a, eth4b, eth5a, or eth5b</td>
<td>eth4a-eth4b</td>
<td>eth5b with eth4a or eth4b</td>
</tr>
<tr>
<td>eth5a with eth5b, eth4a, or eth4b</td>
<td></td>
<td>eth4a with eth4b</td>
</tr>
<tr>
<td>eth5b with eth4a or eth4b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth4a with eth4b</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* a. Single-port optical NICs cannot be used in failover

**Table 3-3: Supported Ethernet Port Pairs, DD OS 4.9 on DD670**

<table>
<thead>
<tr>
<th>Link Aggregation or Failover, 1 GbE Ports</th>
<th>Failover, 10GbE Ports (SFP+ copper and optical)</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0a with eth0b, eth4a, eth4b, eth5a,eth5b,eth1a or eth1b</td>
<td>eth5a with eth5b, eth4a, eth4b, eth1a, or eth1b</td>
</tr>
<tr>
<td>eth0b with eth4a, eth4b, eth5a, eth5b,eth1a or eth1b</td>
<td>eth5b with eth4a, eth4b, eth1a, or eth1b</td>
</tr>
<tr>
<td>eth5a with eth5b, eth4a, eth4b,eth1a or eth1b</td>
<td>eth4a with eth4b, eth1a, or eth1b</td>
</tr>
<tr>
<td>eth5b with eth4a, eth4b, eth1a or eth1b</td>
<td>eth4b with eth1a, or eth1b</td>
</tr>
<tr>
<td>eth4a with eth4b,eth1a or eth1b</td>
<td>eth1a with eth1b</td>
</tr>
</tbody>
</table>
Table 3-3: Supported Ethernet Port Pairs, DD OS 4.9 on DD670

<table>
<thead>
<tr>
<th>Link Aggregation or Failover, 1 GbE Ports</th>
<th>Failover, 10GbE Ports (SFP+ copper and optical)</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth4b with eth1a or eth1b</td>
<td></td>
</tr>
<tr>
<td>eth1a with eth1b</td>
<td></td>
</tr>
</tbody>
</table>

Table 3-4: Supported Ethernet Port Pairs, DD OS 4.9 on DD660/690

<table>
<thead>
<tr>
<th>Link Aggregation or Failover, 1 GbE Ports</th>
<th>Failover, 10 GbE Ports (Dual-port CX4 copper only, no single-port optical(^a))</th>
<th>Failover, 10GbE Ports (Dual-port SFP+ copper and optical)</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0a with eth0b, eth6a, eth6b, eth5a, or eth5b</td>
<td>eth5a-eth5b</td>
<td>eth6a with eth6b, eth5a, or eth5b</td>
</tr>
<tr>
<td>eth0b with eth6a, eth6b, eth5a, or eth5b</td>
<td>eth6a-eth6b</td>
<td>eth6b with eth5a or eth5b</td>
</tr>
<tr>
<td>eth6a with eth6b, eth5a, or eth5b</td>
<td></td>
<td>eth5a with eth5b</td>
</tr>
<tr>
<td>eth6b with eth5a or eth5b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth5a with eth5b</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\(^a\) Single-port optical NICs cannot be used in failover

Where Slot-based Port Naming is Used

Platforms that support slot-based port naming in DD OS 4.9:

- All new platforms, DD670 and later (these platforms only have only slot-based port naming support available).
- Some pre-DD OS 4.9 deployed platforms have the capacity to support both pre-DD OS 4.9 naming and slot-based port naming. Slot-based port naming is enabled on a fresh install:
  - DD140, DD610, DD630, DD660, DD690, DD690g, DD880, DD880g
Platforms that do not support slot-based port naming on DD OS 4.9:

- DD5xx
- DD4xx
- DD120

### Create a Virtual Interface

Virtual interfaces used for failover or link aggregation must be created from pairs that are supported for the kind of interface you are creating, as specified in Table 3-1 on page 34.

- 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, you need to create virtual interfaces from identical physical interfaces, that is, copper to copper, optical to optical, 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 on the same subnet and on the same LAN, or for legacy cards, 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:

1. **Use the net create virtual command. Enter:**
   
   ```
   # net create virtual vethx
   ```
   
   where `x` is decimal or hexadecimal numbers (0-9 and aA-fF) that is a unique identifier for the virtual interface.

2. **Assign the virtual interface an IP address and optional netmask. Enter:**
## Configure Failover

Some considerations for configuring failover:

- A maximum of five Ethernet ports can be configured as virtual interfaces for failover.

- For systems shipped before DD OS 4.9, 10 GbE-to-10 GbE copper ports only: Because ports eth0 and eth1 are reserved for the motherboard, only the physical interfaces (eth2 and eth3 or eth4 and eth5) can be configured for failover in a virtual interface.

- For systems that shipped with DD OS 4.9 containing Intel cards, failover can be configured across cards provided they are of the same type (for example, if both the optional 10 GbE cards are Intel 10 GbE, then all four ports can be grouped for failover).

- A physical port cannot already be configured for VLAN.

To configure failover:

1. Create a virtual interface and assign it an IP address. See Create a Virtual Interface on page 38 for instructions.

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

   ```
   # net disable iname
   
   where iname 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 physical ports. To assign one of the physical interfaces as the primary failover interface, use the optional primary parameter. Enter:

   ```
   # net config iname ipaddr [netmask mask]
   ```

   **Note:** DHCP is not supported for virtual interfaces, so the IP address must be assigned.
# net failover add virtual-ifname interfaces physical-port-list [primary physical-port]

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

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

This output displays:

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

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

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

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

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

```
# net failover show
```

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

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

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

This output displays:

```
Interfaces for veth1: eth4a, eth4b, eth5a
```

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

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

## Configure Link Aggregation

The `net aggregate` command enables a virtual interface for link aggregation with the specified physical interfaces with one of three aggregation modes. Select the mode that is compatible with the switch in use:
• roundrobin
Transmits packets in sequential order from the first available link through the last in the aggregated group.
• xor-L2
Transmits packets based on static balanced mode aggregation with an XOR hash of Layer 2 (inbound and outbound MAC addresses).
• xor-L3L4
Transmits packets based on static balanced mode aggregation with an XOR hash of Layer 3 (inbound and outbound IP address) and Layer 4 (inbound and outbound port numbers).

Some considerations for configuring link aggregation:
• A maximum of four Ethernet ports can be configured as interfaces for link aggregation.
• A physical port cannot already be configured for VLAN.
• The 10 GbE-to-10 GbE interface does not support link aggregation. Only 1 GbE ports are supported.
• All physical ports in the link aggregation group must be connected to the same switch.

To configure link aggregation:
1. Create a virtual interface and assign it an IP address. See Create a Virtual Interface on page 38 for instructions.
2. Disable each of the physical ports that you plan to use as aggregation interfaces. Enter:

```
# net disable ifname
```
where *ifname* is the port name. For example, for eth2a and eth2b:

```
# net disable eth2a
# net disable eth2b
```
3. Create an aggregate virtual interface by specifying the physical ports and mode (the mode must be specified). Choose the
mode that is compatible with the requirements of the switch to which the ports are directly attached. Enter:

```
# net aggregate add virtual-ifname mode {xor-L2 | xor-L2 | roundrobin} interfaces physical-port-list
```

For example, to create an aggregate virtual interface `veth1` from the two physical interfaces `eth2a` and `eth2b`, using the mode xor-L2, enter:

```
# net aggregate add veth1 mode xor-L2 interfaces eth2a eth2b
```

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

```
# 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, aggregation mode, and the ports that comprise the virtual interface.

## Configure VLAN Tagging

To configure VLAN tagging:

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

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

```
# net config eth5b up
```

3. Create the VLAN interface using either a physical port or a configured virtual port (to create the virtual port, see Create a Virtual Interface on page 38). The range for `vlan-id` is between 1 and 4098:
# net create interface \( \{ \text{physical-ifname} \mid \text{virtual-ifname} \} \) vlan vlan-id

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

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

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

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

```bash
# net config ifname ipaddr netmask 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.

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

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

```bash
# net show settings
```

<table>
<thead>
<tr>
<th>port</th>
<th>enabled</th>
<th>DHCP</th>
<th>IP address</th>
<th>netmask</th>
<th>additional setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth5b.1</td>
<td>yes</td>
<td>no</td>
<td>192.168.11.156</td>
<td>255.255.252.0</td>
<td></td>
</tr>
</tbody>
</table>

The abridged output above shows the name of the VLAN interface (eth2.1), whether or not it is enabled, if it uses DHCP, its IP address and netmask, and the full VLAN:port specifier.

### Additional Physical or Virtual Interface Configuration

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

#### Specify the MTU

You can set the MTU size for a physical or virtual interface, or a vlan interface (as long as it is less then or equal to the underlining base interface MTU value). Supported maximum transfer unit size
values range from 1500 to 9014. For 100 Base-T and gigabit networks, 1500 is the default.

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

Note: All of your network components need to support the size that you set.

Enter:

```bash
# net config iface mtu {size | default}
```

where `iface` is the name of the interface.

## Configure Duplex Line Use and Speed

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

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

- Have the network interface card automatically negotiate these settings for an interface.

Note: The following restrictions apply:

- Duplex line use and auto-negotiate do not apply to 10 GbE cards.

- A line speed of 1000 must have a full-duplex setting.

### Set an Interface’s Duplex Line Use

Enter:

```bash
# net config iface duplex {full|half} speed {10 | 100 | 1000}
```

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

```bash
# net config veth1 duplex half speed 100
```
Set Auto-negotiate for an Interface

1. Enter:

   
   `# net config ifname autoneg`

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

   `# net config eth1a autoneg`

Routing Tables and Gateways

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

`# route show table`

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

Configuring SNMP on a Data Domain System

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

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

Add a Community String

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

   
   `# snmp add rw-community community-string`
   `# snmp add ro-community community-string`
For example, to add a community string of `private` with read/write permissions, enter:

```sh
# snmp add rw-community private
```

## Enable SNMP

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

As an administrator, enter:

```sh
# snmp enable
```

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

## Set the System Location

As an administrator, enter:

```sh
# snmp set sysLocation location
```

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

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

## Set a System Contact

As an administrator, enter:

```sh
# snmp set sysContact contact
```

This command sets the system contact as used in the SNMP MIB II system variable `sysContact`, such as a contact of `bob-smith`:

```sh
# snmp set sysContact bob-smith
```

**Note:** The SNMP `sysContact` variable is not the same as that set using the `config set admin-email` command. If the SNMP variables are not set with the `snmp` commands, the variables default to the system values given as part of the `config set` commands.
Add a Trap Host

As an administrator, enter:

```
# snmp add trap-host host[:port]
```

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
```

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

Configuring SOL for IPMI

You can use the Intelligent Platform Management Interface (IPMI) to power up, power down, or power cycle a Data Domain system in a remote location from a host Data Domain system, if both systems support this standard.

The Serial-Over-LAN (SOL) feature of IPMI is used to view the serial output of a remote system’s boot sequence.

Follow the steps below to set up an SOL connection.

1. If the Data Domain controller on which you are activating SOL is listed below, adjust the BIOS settings as instructed. Otherwise, proceed to the next step.

<table>
<thead>
<tr>
<th>Appliance</th>
<th>BIOS Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>DD890, DD860, DD670</td>
<td>Go to Server &gt; Set BMC IP address source &gt; DHCP.</td>
</tr>
<tr>
<td>DD120, DD5xx, DD660, DD690</td>
<td>Press F2 to go to BIOS.  &lt;br&gt;• Advanced &gt; Serial Port Configuration &gt; Serial B Enable [Enabled].  &lt;br&gt;• Server Management &gt; Console Redirection &gt; Serial Port B &gt; Baud Rate 9.6K</td>
</tr>
</tbody>
</table>
2. Run `system option set console` to modify the GRUB console setting.

3. When prompted, enter `yes` to reboot the system.

4. Run `ipmi remote console` to activate the SOL connection.

5. To disconnect from an SOL session and return to the command line, use the symbol `@`.

On most supported Data Domain controllers, the SOL bit rate is 9600 bps.

**Note:** Following a BIOS upgrade, reset the BIOS setting for SOL usage.

For instructions on using the SOL feature, see the `ipmi` command in the *DD OS 5.0 Command Reference Guide*.

## Configuring Encryption of Data at Rest

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

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

To learn more about how the Encryption at Rest feature works, and to view configuration and management procedures, refer to the section “Managing Encryption at Rest” in the “Managing the File System” chapter of the *DD OS 5.0 Administration Guide*.

## Optional Configuration Procedures

You can perform the following tasks now or later. See the *DD OS 5.0 Administration Guide* for more information.

- Add users
• Enable FTP and Telnet for data access
• Add remote hosts that can use FTP or Telnet
• Add email addresses to receive system reports
4   Adding Expansion Shelves and Third-Party LUNs

This chapter covers the following topics:

- Adding Expansion Shelves on page 51
- Adding a Third-Party LUN to a Gateway Systems on page 53

Adding Expansion Shelves

Install the new expansion shelf as described in the Data Domain Expansion Shelf Hardware Guide. The procedure described here, which adds shelves to the volume and creates RAID groups, applies only to adding a new expansion shelf to an active Data Domain system.

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

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

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

   # disk port show summary

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

2. Verify that the Data Domain system recognizes the shelves by entering:

   # enclosure show summary

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

Add Enclosure Disks to the Volume

1. Enter:

   # storage add enclosure enclosure-id

   where enclosure-id is always 2 for the first added shelf and 3 for the second.

   **Note:** The Data Domain system always has the 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. Type y.

3. When prompted, enter your sysadmin password.

4. (Optional) Add disks in another enclosure at this time by entering:

   # storage add enclosure enclosure

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

   # storage show all
Two disks in a shelf are spare disks. The rest should report that they are in use.

**Disks Labeled Unknown Instead of Spare**

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

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

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

   ```
   # filesys status
   ```

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

   ```
   # filesys show space
   ```

**Adding a Third-Party LUN to a Gateway Systems**

Follow the procedures described below.

*Warning:* After you add a LUN, it cannot be removed without loss of data.

**Create and Verify the New LUN**

1. Create a new LUN on the third-party physical disk storage as directed by the third-party provider’s instructions. The masking set for the new LUN must allow the Data Domain system to recognize it.

2. On the Data Domain system, verify the new LUN by entering:

   ```
   # disk rescan
   ```

   The output should state that a new device was found.
**Note:** If there are previously configured LUNS, entering the `disk show raid-info` command shows these LUNS as in use, and the new LUN as unknown and not in use.

## Add the LUN to the Data Domain File System

1. Enter:
   ```
   # storage add devID
   
   For example, storage add dev3.
   ```

2. Because the newly added LUN (disk) cannot be removed from the file system without re-installing the Data Domain operation system, you are prompted to confirm that you want to add this disk. Type `y`.

3. To verify that the new LUN is in use, enter:
   ```
   # storage show all
   ```
A Time Zones

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

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

Examples of time zones include:

- GMT+5
- Europe/Stockholm
- US/Pacific
- Chile/EasterIsland
- Japan
### Africa

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

### America

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

### Antarctica

<table>
<thead>
<tr>
<th>Antarctica/Casey</th>
<th>Antarctica/DumontDUrville</th>
<th>Antarctica/Mawson</th>
<th>Antarctica/McMurdo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antarctica/Palmer</td>
<td>Antarctica/South_Pole</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Asia

<table>
<thead>
<tr>
<th>Asia/Aden</th>
<th>Asia/Alma-Ata</th>
<th>Asia/Amman</th>
<th>Asia/Anadyr</th>
<th>Asia/Aqtau</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia/Aqtobe</td>
<td>Asia/Ashkhabad</td>
<td>Asia/Baghdad</td>
<td>Asia/Bahrain</td>
<td>Asia/Baku</td>
</tr>
<tr>
<td>Asia/Bangkok</td>
<td>Asia/Beirut</td>
<td>Asia/Bishkek</td>
<td>Asia/Brunei</td>
<td>Asia/Calcutta</td>
</tr>
<tr>
<td>Asia/Chungking</td>
<td>Asia/Colombo</td>
<td>Asia/Dacca</td>
<td>Asia/Damascus</td>
<td>Asia/Dubai</td>
</tr>
<tr>
<td>Asia/Dushanbe</td>
<td>Asia/Gaza</td>
<td>Asia/Harbin</td>
<td>Asia/Hong_Kong</td>
<td>Asia/Irkutsk</td>
</tr>
<tr>
<td>Asia/Ishigaki</td>
<td>Asia/Istanbul</td>
<td>Asia/Jakarta</td>
<td>Asia/Jayapura</td>
<td>Asia/Jerusalem</td>
</tr>
<tr>
<td>Asia/Kabul</td>
<td>Asia/Kamchatka</td>
<td>Asia/Karachi</td>
<td>Asia/Kashgar</td>
<td>Asia/Katmandu</td>
</tr>
<tr>
<td>Asia/Krasnoyarsk</td>
<td>Asia/Kuala_Lumpur</td>
<td>Asia/Kuching</td>
<td>Asia/Kuwait</td>
<td>Asia/Macao</td>
</tr>
<tr>
<td>Asia/Magadan</td>
<td>Asia/Manila</td>
<td>Asia/Muscat</td>
<td>Asia/Nicosia</td>
<td>Asia/Novosibirsk</td>
</tr>
<tr>
<td>Asia/Omsk</td>
<td>Asia/Phnom_Penh</td>
<td>Asia/Pyongyang</td>
<td>Asia/Qatar</td>
<td>Asia/Rangoon</td>
</tr>
<tr>
<td>Asia/Riyadh</td>
<td>Asia/Reigon</td>
<td>Asia/Seoul</td>
<td>Asia/Shanghai</td>
<td>Asia/Singapore</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Time Zone</td>
<td>Time Zone</td>
<td>Time Zone</td>
<td>Time Zone</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------</td>
<td>--------------------</td>
<td>--------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Asia/Taipei</td>
<td>Asia/Tashkent</td>
<td>Asia/Tbilisi</td>
<td>Asia/Tehran</td>
<td>Asia/Tel_Aviv</td>
</tr>
<tr>
<td>Asia/Thimbu</td>
<td>Asia/Tokyo</td>
<td>Asia/Ujung_Pandang</td>
<td>Asia/Ulan_Bator</td>
<td>Asia/Urumqi</td>
</tr>
<tr>
<td>Asia/Vientiane</td>
<td>Asia/Vladivostok</td>
<td>Asia/Yakutsk</td>
<td>Asia/Yekaterinburg</td>
<td>Asia/Yerevan</td>
</tr>
</tbody>
</table>

**Atlantic**

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

**Australia**

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

**Brazil**

<table>
<thead>
<tr>
<th>Time Zone</th>
<th>Time Zone</th>
<th>Time Zone</th>
<th>Time Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brazil/Acre</td>
<td>Brazil/DeNoronha</td>
<td>Brazil/East</td>
<td>Brazil/West</td>
</tr>
</tbody>
</table>

**Canada**

<table>
<thead>
<tr>
<th>Time Zone</th>
<th>Time Zone</th>
<th>Time Zone</th>
<th>Time Zone</th>
<th>Time Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada/Atlantic</td>
<td>Canada/Central</td>
<td>Canada/East-Saskatchewan</td>
<td>Canada/Eastern</td>
<td></td>
</tr>
<tr>
<td>Canada/Mountain</td>
<td>Canada/Newfoundland</td>
<td>Canada/Pacific</td>
<td>Canada/Saskatchewan</td>
<td></td>
</tr>
<tr>
<td>Canada/Yukon</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chile

Chile/Continental  Chile/EasterIsland

Etc

Etc/GMT  Etc/GMT+0  Etc/GMT+1  Etc/GMT+2  Etc/GMT+3
Etc/GMT+4  Etc/GMT+5  Etc/GMT+6  Etc/GMT+7  Etc/GMT+8
Etc/GMT+9  Etc/GMT+10  Etc/GMT+11  Etc/GMT+12  Etc/GMT+13
Etc/GMT+14  Etc/GMT+15

Etc/GMT-0  Etc/GMT-1  Etc/GMT-2  Etc/GMT-3  Etc/GMT-4
Etc/GMT-5  Etc/GMT-6  Etc/GMT-7  Etc/GMT-8  Etc/GMT-9
Etc/GMT-10  Etc/GMT-11  Etc/GMT-12  Etc/GMT-13  Etc/GMT-14
Etc/GMT-15

Etc/Greenwich  Etc/UCT  Etc/Universal  Etc/UTC  Etc/Zulu

Europe

Europe/Amsterdam  Europe/Andorra  Europe/Athens  Europe/Belfast  Europe/Belgrade
Europe/Berlin  Europe/Bratislava  Europe/Brussels  Europe/Bucharest  Europe/Budapest
Europe/Chisinau  Europe/Copenhagen  Europe/Dublin  Europe/Gibraltar  Europe/Helsinki
Europe/Istanbul  Europe/Kiev  Europe/Kuybysh  Europe/Lisbon  Europe/Ljubljana
Europe/London  Europe/Luxembourg  Europe/Madrid  Europe/Malta  Europe/Minsk
Europe/Monaco  Europe/Moscow  Europe/Oslo  Europe/Paris  Europe/Prague
Europe/Riga  Europe/Rome  Europe/San Marino  Europe/Sarajevo  Europe/Simferopol
Europe/Skopje  Europe/Sofia  Europe/Stockholm  Europe/Tallinn  Europe/Tirane
Europe/Vaduz  Europe/Vatican  Europe/Vienna  Europe/Vilnius  Europe/Warsaw
Europe/Zagreb  Europe/Zurich
## GMT

<table>
<thead>
<tr>
<th></th>
<th>GMT</th>
<th>GMT+1</th>
<th>GMT+2</th>
<th>GMT+3</th>
<th>GMT+4</th>
<th>GMT+5</th>
<th>GMT+6</th>
<th>GMT+7</th>
<th>GMT+8</th>
<th>GMT+9</th>
<th>GMT+10</th>
<th>GMT+11</th>
<th>GMT+12</th>
<th>GMT+13</th>
<th>GMT+14</th>
</tr>
</thead>
</table>

### Indian (Indian Ocean)

<table>
<thead>
<tr>
<th></th>
<th>Indian/Antananarivo</th>
<th>Indian/Chagos</th>
<th>Indian/Christmas</th>
<th>Indian/Cocos</th>
<th>Indian/Comoro</th>
<th>Indian/Kerguelen</th>
<th>Indian/Mahe</th>
<th>Indian/Maldives</th>
<th>Indian/Mauritius</th>
<th>Indian/Mayotte</th>
<th>Indian/Reunion</th>
</tr>
</thead>
</table>

### Mexico

<table>
<thead>
<tr>
<th></th>
<th>Mexico/BajaNorte</th>
<th>Mexico/BajaSur</th>
<th>Mexico/General</th>
</tr>
</thead>
</table>

### Miscellaneous

<table>
<thead>
<tr>
<th></th>
<th>Arctic/Longyearbyen</th>
<th>CET</th>
<th>CST6CDT</th>
<th>Cuba</th>
<th>EET</th>
<th>Egypt</th>
<th>Eire</th>
<th>EST</th>
<th>EST5EDT</th>
<th>Factory</th>
<th>GB</th>
<th>GB-Eire</th>
<th>Greenwich</th>
<th>Hongkong</th>
<th>HST</th>
<th>Iceland</th>
<th>Iran</th>
<th>Israel</th>
<th>Jamaica</th>
<th>Japan</th>
<th>Kwajalein</th>
<th>Libya</th>
<th>MET</th>
<th>MST</th>
<th>MST7MDT</th>
<th>Navajo</th>
<th>NZ</th>
<th>NZ-CHAT</th>
<th>Poland</th>
<th>Portugal</th>
</tr>
</thead>
</table>
Pacific

Pacific/Apia Pacific/Auckland Pacific/Chatham Pacific/Easter Pacific/Efate
Pacific/Enderbury Pacific/Fakaofo Pacific/Fiji Pacific/Funafuti Pacific/Galapagos
Pacific/Kiritimati Pacific/Kosrae Pacific/Kwajalein Pacific/Majuro Pacific/Marquesas
Pacific/Midway Pacific/Nauru Pacific/Niue Pacific/Norfolk Pacific/Noumea
Pacific/Pago_Pago Pacific/Palau Pacific/Pitcairn Pacific/Ponape Pacific/Port_Moresby
Pacific/Rarotonga Pacific/Saipan Pacific/Samoan Pacific/Tahiti Pacific/Tarawa
Pacific/Tongatapu Pacific/Truk Pacific/Wake Pacific/Wallis Pacific/Yap

System V

systemV/AST4 systemV/AST4ADT systemV/CST6 systemV/CST6CDT systemV/EST5
systemV/EST5EDT systemV/HST10 systemV/MST7 systemV/MST7MDT systemV/PST8
systemV/PST8PDT systemV/YST9 systemV/YST9YDT

US (United States)

US/Pacific US/Pacific-New US/Samoan
Aliases

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