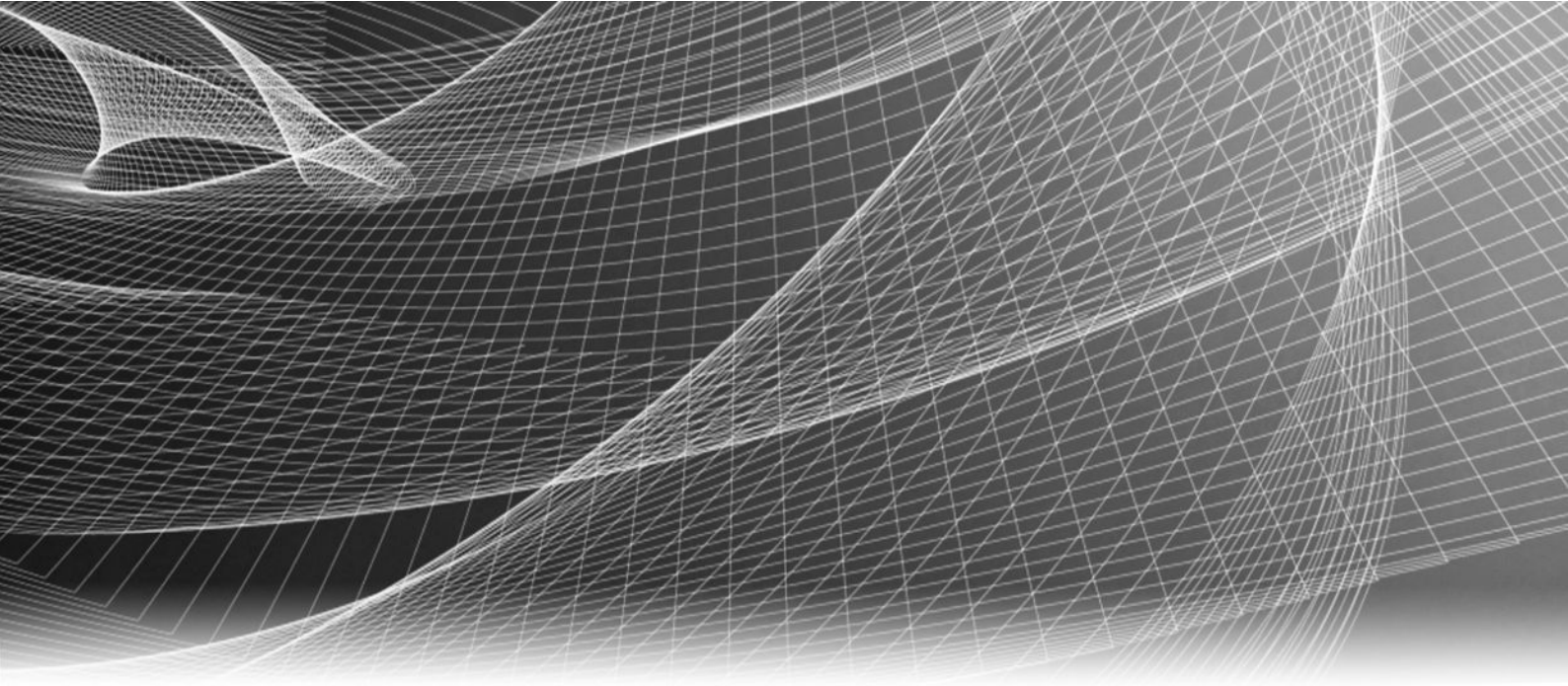

EMC Data Domain Operating System

Version 5.5

Command Reference Guide

302-000-476

REV. 05

EMC²

Published April, 2015

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

FIGURES

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 EMC Online Support (https://support.emc.com) to ensure that you are using the latest version of this document.

Purpose

This guide describes the EMC Data Domain operating system (DD OS) commands and provides an overview of how they are used. For more specific, task-based instructions, see the *EMC Data Domain Operating System Administration Guide*.

Related documentation

The following Data Domain system documents provide additional information.

- Installation and setup guide for your system, for example, *EMC Data Domain DD 2500 Storage System, Installation and Setup Guide*
- *EMC Data Domain Operating System USB Installation Guide*
- *EMC Data Domain Operating System DVD Installation Guide*
- *EMC Data Domain Operating System Release Notes*
- *EMC Data Domain Operating System Initial Configuration Guide*
- *EMC Data Domain Product Security Guide*
- *EMC Data Domain Operating System Administration Guide*
- *EMC Data Domain Operating System MIB Quick Reference*
- *EMC Data Domain Operating System Offline Diagnostics Suite User's Guide*
- Hardware overview guide for your system, for example, *EMC Data Domain DD4200, DD4500, and DD7200 Systems, Hardware Overview*
- Field replacement guides for your system components, for example, *Field Replacement Guide, Data Domain DD4200, DD4500, and DD7200 Systems, IO Module and Management Module Replacement or Upgrade*
- *EMC Data Domain, System Controller Upgrade Guide*
- *EMC Data Domain Expansion Shelf, Hardware Guide* (for shelf model ES20 or ES30)
- *EMC Data Domain Boost for OpenStorage Administration Guide*
- *EMC Data Domain Boost for Oracle Recovery Manager Administration Guide*
- *EMC Data Domain Boost SDK Programmer's Guide*
- *Statement of Volatility for the Data Domain DD2500 System*
- *Statement of Volatility for the Data Domain DD4200, DD4500, or DD7200 System*

Special notice conventions used in this document

EMC uses the following conventions for special notices.

NOTICE

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

Note

A note identifies information that is incidental, but not essential, to the topic. Notes can provide an explanation, a comment, reinforcement of a point in the text, or just a related point.

Typographical conventions

The following table describes the type style conventions used in this document.

Table 1 Typographical Conventions

Bold	Use for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)
Italic	Use for full titles of publications referenced in text
`Monospace`	Use for: • System code • System output, such as an error message or script • Pathnames, filenames, prompts, and syntax • Commands and options
`Monospace italic`	Use for variables
`Monospace bold`	Use for user input
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections - the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

Where to get help

EMC support, product, and licensing information can be obtained from the following sources.

Product information

For documentation, release notes, software updates, or information about EMC products, go to EMC Online Support at https://support.emc.com.

EMC Data Domain product documentation

To view documentation for EMC Data Domain products, go to EMC Online Support and click Support by Product below the Search box. Type **`Data Domain`** in the Find a Product box, wait for those words to appear in the list of matches below the box, and click the words. Then click ››. In the list of categories under the Search box, click Documentation.

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

Technical support

Go to EMC Online Support and click Service Center. You will see several options for contacting EMC Technical Support. Note that to open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

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: DPAD.Doc.Feedback@emc.com.

Revision History

Table 2 Document Revision History

Revision	Date	Description
05 (5.5.2.0)	January 2015	New `system passphrase` commands are added to manage the minimum length, and the output of `system show performance` now shows columns for replication in and replication out streams. The `filesys encryption` commands have been modified to display messages that the commands do not affect offline archive tiers, and offline archive units. The `route del` command description is updated. SNMP version support is defined in the guidelines for the SNMP command. New `ddboost` commands are added to support the renaming and undeleting of storage units. The `ddboost ifgroup add` and `ddboost ifgroup del` commands have been modified to accommodate IPv6 addresses. The `ddboost storage-unit create` and `ddboost storage-unit modify` commands have been modified to include the `report-physical-size` argument. The commands for mtree option set and reset of app-optimized compression (Oracle Optimized Deduplication) have been added.
04 (5.5.1.4)	December 2014	Updated the `config set timezone` command description and added an appendix with changes to the supported timezones.
03 (5.5.1.3)	November 2014	The syntax is changed for the commands to set and reset the DDNS TSIG key. See the `net ddns` command descriptions for more information.
02 (5.5.1)	October 2014	Kerberos authentication commands and options have been added. Many `filesys encryption` commands have been enhanced to support the use of Encryption of Data at Rest with DD Extended Retention-enabled Data Domain systems. The `net ddns` commands have been updated to support DDNS in both the Windows and UNIX environments. IPv6 support is expanded to enable operation in IPv6 only environments. DD OS now supports IPv6 address use with DHCP, DNS, and DDNS. Multiple IPv6 addresses are supported on an interface using aliases. Affected commands are `net config` and `net create interface`. The `system show all` and `system show serialno` commands now display the product serial number instead of the chassis serial number for newer systems.

Table 2 Document Revision History (continued)

Revision	Date	Description
		Additional updates are described in the “Change History” for each command.
01	May 2014	Commands have been added to add and delete clients with IPv6 addresses. See the NFS chapter. Support has been added for separate host certificates for HTTPS, RSA Key Manager, and DD Boost clients. CA certificate support has been provided for RSA Key Manager and DD Boost clients. The role(s) required for each command have been added to each command description. VTL now includes support for IBM LTO-5, i60000, and DDVTL (a generic tape library). A chapter has been added for the new Secure Multi-Tenancy (smt) feature. A chapter has been added for the new Virtual Disk Device (vdisk) feature. Additional updates are described in the “Change History” for each command.

CHAPTER 1

adminaccess

The `adminaccess` command manages access control and enables users to import host and CA certificates. Command options also enable remote hosts to use the FTP, FTPS, Telnet, HTTP, HTTPS, SSH, and SCP administrative protocols on the Data Domain system. SSH is open to the default user sysadmin and to users added by the administrator.

A Certificate Signing Request (CSR) can now be generated for a host certificate. Also, host certificates can now be imported in PKCS12 or PEM formats. EMC Data Domain uses the SHA1 RSA encryption algorithm for a CSR and PBE-SHA1-3DES encryption algorithm for the PKCS12 key and certificate.

This chapter contains the following topics:

adminaccess Change History

This section provides a list of changes since the 5.4 release, for all 5.5.x releases, in order of most recent release to first release.

New Commands in DD OS 5.5

adminaccess certificate cert-signing-request delete
Delete the certificate signing request.

adminaccess certificate cert-signing-request show
Show the certificate signing request stored on the system.

adminaccess certificate export imported-ca {subject *subject-name* | fingerprint *fingerprint*} [file *file-name*]
Export a CA certificate for the specified subject name or fingerprint.

adminaccess certificate export imported-ca-for-host application {ddboost | rkm | *application-list*} [file *file-name*]
Export a CA certificate for the specified host applications.

Modified Arguments in DD OS 5.5

adminaccess certificate generate cert-signing-request [key-strength {1024bit | 2048bit | 4096bit}] [country *country-code*] [state *state*] [city *city*] [org-name *organization-name*] [org-unit *organization-unit*] [common-name *common-name*]
Moved `generate` keyword, and added 3072 bit key-strength option. New syntax:
`adminaccess certificate cert-signing-request generate [key-strength {1024bit | 2048bit | 3072bit | 4096bit}] [country *country-code*] [state *state*] [city *city*] [org-name *organization-name*] [org-unit *organization-unit*] [common-name *common-name*]`

adminaccess certificate delete {imported-host | imported-ca | support-bundle-ca | subject *subject-name* | fingerprint *fingerprint*}
Two new command variations enable deletion of certificates per application:
`adminaccess certificate delete {imported-host application {all | ddboost | https | rkm | *application-list*} | imported-ca application {all | ddboost | rkm | support | *application-list*}}`
`adminaccess certificate delete {subject *subject-name* | fingerprint *fingerprint*} [application {all | ddboost | https | rkm | support | *application-list*}]`

adminaccess certificate import {host | ca} [file *file-name*]
This command option now supports certificate import to one or more applications:
`adminaccess certificate import {host application {all | ddboost | https | rkm | *application-list*} | ca application {all | ddboost | rkm | *application-list*}} [file *file-name*]`

adminaccess certificate show [detailed] [host | imported-host | ca | imported-ca | support-bundle-ca | cert-signing-request]

This command option now supports certificate display for one or more applications: `adminaccess certificate show [detailed] [imported-host [application {all | ddboost | https | rkm | application-list}] | imported-ca [application {all | ddboost | rkm | support | application-list}] | host | ca | subject subject-name | fingerprint fingerprint`

adminaccess Guidelines and Restrictions

- FTP and FTPS are mutually exclusive. Only one or the other can be enabled, not both.
- SCP can be enabled only when SSH is enabled.
- FTP and Telnet are disabled by default.

adminaccess add

`adminaccess add ssh-keys [user username]`

Add an SSH public key created on a UNIX-based remote machine to the SSH authorized keys file on the Data Domain system. Role required: admin, security, user, backup-operator, or none.

adminaccess authentication

`adminaccess authentication add {cifs}`

Allow Windows domain users with no local account on the Data Domain system to access the system through SSH, Telnet, and FTP using Windows domain group credentials. For administrative access, the user must be in the standard Windows Domain Admins group or in a group that you create named Data Domain. Users from both group names are always accepted as administrative users. The command also gives user-level access (no administrative operations allowed) to all other users from the domain. Users must be from the domain that includes the Data Domain system or a related, trusted domain.

The SSH, Telnet, or FTP command that accesses the Data Domain system must include the domain name, a backslash, and the user name in double quotation marks.

Note

CIFS must be enabled and the Data Domain system must be part of a Windows domain.

Role required: admin.

`adminaccess authentication del {cifs}`

Prevent authentication of a Windows domain. Allow admin role only for users with local user accounts on the Data Domain system. Role required: admin.

`adminaccess authentication reset {cifs}`

Reset the Windows user access to the default of requiring a local account for administrative access to the Data Domain system. Role required: admin.

`adminaccess authentication show`

Display whether CIFS authentication is enabled or disabled. Role required: admin, security, user, or backup-operator.

adminaccess certificate

`adminaccess certificate cert-signing-request delete`
Delete the certificate signing request. To see if there is a certificate signing request on the system, enter `adminaccess certificate cert-signing-request show`. Role required: admin.

`adminaccess certificate cert-signing-request generate [key-strength {1024bit | 2048bit | 3072bit | 4096bit}] [country` *`country-code`*`] [state` *`state`*`] [city` *`city`*`] [org-name` *`organization-name`*`] [org-unit` *`organization-unit`*`] [common-name` *`common-name`*`]`
Generate a Certificate Signing Request (CSR) file at the following path `/ddvar/certificates/CertificateSigningRequest.csr`. Use SCP, FTP or FTPS to transfer the CSR file from the system to a computer from which you can send the CSR to a Certificate Authority (CA). After you receive a signed CSR file from a CA, you can import the certificate using `adminaccess certificate import`.

If a previously generated CSR exists, the system prompts you to approve or reject certificate regeneration, which replaces the existing CSR.

If the user does not specify values, default values are used.

Note

You must configure a system passphrase (`system passphrase set`) before you can generate a CSR.

Role required: admin.

Argument Definitions
If the value you set for a variable includes any space characters, enclose the variable string in quotes.

key strength
Enumeration values allowed are 1024 bit, 2048 bit, 3072 bit, or 4096 bit. Default is 2048 bit.

country
Default is US. Abbreviation for country cannot exceed two characters. No special characters are allowed.

state
Default is California. Maximum entry is 128 characters.

city
Default is Santa Clara. Maximum entry is 128 characters.

org-name
Default is My Company Ltd. Maximum entry is 64 characters.

org-unit
Default value is empty string. Maximum entry is 64 characters.

common name
Default value is the system host name. Maximum entry is 64 characters.

`adminaccess certificate cert-signing-request show`
Show the certificate signing request stored on the system. Role required: admin, security, user, backup-operator, or none.

`adminaccess certificate delete {imported-host application {all | ddboost | https | rkm | application-list} | imported-ca application {all | ddboost | rkm | support | application-list}}`
Delete a certificate for the specified application.

Note

Log out from the browser session before deleting an HTTPS host certificate. Otherwise HTTPS browser sessions (using imported host certificates) will be closed. After deleting the host certificate, refresh or restart the browser to proceed.

Role required: admin.

Argument Definitions
If the value you set for a variable includes any space characters, enclose the variable string in quotes.

all
Deletes the certificates for all applications.

application-list
To delete the certificates for multiple applications, replace *application-list* with the application names, separated by commas or spaces (for example, **ddboost, rkm**).

ddboost
Deletes the certificate for the DD Boost application.

https
Deletes the certificate for the HTTPS application.

rkm
Deletes the certificate for the RSA Key Manager (RKM) application.

support
Deletes the certificate for the support application.

`adminaccess certificate delete { subject subject-name | fingerprint fingerprint} [application {all | ddboost | https | rkm | support | application-list}]`
Delete a certificate for the specified subject, fingerprint, or application.

Note

Log out from the browser session before deleting an HTTPS host certificate. Otherwise HTTPS browser sessions (using imported host certificates) will be closed. After deleting the host certificate, refresh or restart the browser to proceed.

Role required: admin.

Argument Definitions
If the value you set for a variable includes any space characters, enclose the variable string in quotes.

all
Deletes the certificates for all applications.

application-list
To delete the certificates for multiple applications, replace *application-list* with the application names, separated by commas or spaces (for example, **ddboost, rkm**).

ddboost
Deletes the certificate for the DD Boost application.

fingerprint
Specifies the fingerprint of a certificate to be deleted. To display the available certificates and their footprints, enter `adminaccess certificate show`.

https
Deletes the certificate for the HTTPS application.

rkm
Deletes the certificate for the RSA Key Manager (RKM) application.

subject
Specifies the subject name of a certificate to be deleted. To display the available certificates and their subject names, enter `adminaccess certificate show`.

support
Deletes the certificate for the support application.

`adminaccess certificate export imported-ca {subject` *`subject-name`* `| fingerprint` *`fingerprint`*`} [file` *`file-name`*`]`
Export a CA certificate for the specified subject name or fingerprint. The certificate appears on screen after the CLI command. Role required: admin.

Argument Definitions
If the value you set for a variable includes any space characters, enclose the variable string in quotes.

file
Saves a copy of the certificate in the /ddvar/certificates directory using the specified filename.

fingerprint
Specifies the fingerprint of a certificate to be exported. To display the available certificates and their footprints, enter `adminaccess certificate show`.

subject
Specifies the subject name of a certificate to be exported. To display the available certificates and their subject names, enter `adminaccess certificate show`.

`adminaccess certificate export imported-ca-for-host application {ddboost | rkm |` *`application-list`*`} [file` *`file-name`*`]`
Export a CA certificate for the specified host applications. The certificate appears on screen after the CLI command. Role required: admin.

Argument Definitions
If the value you set for a variable includes any space characters, enclose the variable string in quotes.

application-list
To export the certificates for multiple applications, replace *application-list* with the application names, separated by commas or spaces (for example, **`ddboost, rkm`**).

ddboost
Exports the certificate for the DD Boost application.

rkm
Exports the certificate for the RSA Key Manager (RKM) application.

file
Saves a copy of the certificate in the /ddvar/certificates directory using the specified filename.

`adminaccess certificate import {host application {all | ddboost | https | rkm | application-list} | ca application {all | ddboost | rkm | application-list}} [file file-name]`

Imports a certificate for one or more applications. You can import only one certificate per application, but you can use the same certificate for multiple applications.

To prepare for importing a certificate, use SCP, FTP, or FTPS to copy the host or CA certificate to the directory: `/ddvar/certificates`. Optionally, you can copy and paste the entire PEM file of the host certificate, and then run the import command without specifying the certificate filename. An error is generated if users mistakenly import a mismatched certificate; for example, importing a host certificate as a CA certificate, or vice versa.

Directly importing an RKM auto-registered certificate and bulk importing multiple certificates is not supported. After a public host certificate is imported, any related CSR is deleted from the system.

- Users must provide the PKCS12 file and password to decrypt the PKCS12 file.
- CA certificates must be imported in PEM format.

When importing or deleting certificates on an encrypted Data Domain system on which the system passphrase is set, the imported host PKCS12 certificate is reencrypted with the system passphrase. If the system passphrase is not set, an error is generated during the import.

When the system passphrase is changed, the imported host PKCS12 certificate, if present on Data Domain system, is reencrypted using the new system passphrase.

The correct server or client extensions must also be set. See the sections “Basic Constraints,” “Key Usage,” and “Extended Key Usage” in RFC 5280 for details (http://www.ietf.org/rfc/rfc5280.txt). Extensions are provided for host certificates during the certificate signing process.

Note

When a certificate is imported for HTTPS (which is used by DD System Manager), running this command closes any current browser sessions. It is a good practice to log out of the DD System Manager sessions prior to running this command.

Role required: admin.

Argument Definitions

If the value you set for a variable includes any space characters, enclose the variable string in quotes.

all
Imports the same certificate for all applications.

application-list
To import a certificate for multiple applications, replace *application-list* with the application names, separated by commas or spaces (for example, **`ddboost, rkm`**).

ca application
Indicates that the certificate to be imported is a CA certificate.

ddboost
Imports the certificate for the DD Boost application.

host application
Indicates that the certificate to be imported is a host certificate.

rkm
Imports the certificate for the RSA Key Manager (RKM) application.

file
Specifies a file from which to import the certificate. A copy of the certificate file must be in the /ddvar/certificates directory.

Example 1

On the local system, enter:

```
# scp host.p12 <administrator_role>@<DD>:/ddvar/certificates
```

On the Data Domain system, enter:

```
# adminaccess certificate import host application https file host.p12
```

`adminaccess certificate show [detailed] [imported-host [application {all | ddboost | https | rkm | application-list}] | imported-ca [application {all | ddboost | rkm | support | application-list}] | host | ca | subject subject-name | fingerprint fingerprint`
Display certificates for the imported host, CA, imported CA, or support bundle server trusted CA. All users may run this command option. Role required: admin, security, user, backup-operator, or none.

Argument Definitions
If the value you set for a variable includes any space characters, enclose the variable string in quotes.

all
Displays the certificates in use for all applications.

application-list
Specifies a list of applications for which certificates will be displayed.

ca
Specifies the CA certificates are to be displayed.

ca application
Displays CA certificates for the specified applications.

ddboost
Displays the certificate for the DD Boost application.

fingerprint
Displays the certificate with the specified fingerprint. To display the available certificates and their footprints, enter `adminaccess certificate show`.

host
Specifies the host certificates are to be displayed.

host application
Displays host certificates for the specified applications.

https
Displays the certificate for the HTTPS application.

rkm
Displays the certificate for the RSA Key Manager (RKM) application.

subject
Displays all certificate that use the specified subject. To display the available certificates and their subject names, enter `adminaccess certificate show`.

support
Displays the certificate for the support application.

adminaccess del

`adminaccess del ssh-keys` *`lineno`* `[user` *`username`*`]`
Delete an SSH key from the key file. Users may delete their own keys, and users in admin role may delete user keys. Run the command option adminaccess show ssh-keys to view line number values. Role required: admin, security, user, backup-operator, or none.

adminaccess disable

`adminaccess disable {http | https | ftp | ftps | telnet | ssh | scp | all}`
Disable administrative access on the Data Domain system. Disabling FTP or Telnet does not affect entries in the access lists. If all access is disabled, the Data Domain system is available only through a serial console or keyboard and monitor. Role required: admin.

adminaccess enable

`adminaccess enable {http | https | ftp | ftps | telnet | ssh | scp | all}`
Enable a protocol on the Data Domain system. By default, the SSH, HTTP, and HTTPS services are enabled and FTP and Telnet are disabled. HTTP and HTTPS allow users to log in from System Manager. To use FTP and Telnet, users with admin role permissions must add host machines to the access lists. Role required: admin.

adminaccess ftp

`adminaccess ftp add` *`host-list`*
Add one or more hosts to the FTP list. You can identify a host using a fully qualified hostname, an IPv4 address, or an IPv6 address. Host entries cannot include a space. Multiple entries may be separated by commas, spaces, or both. Role required: admin.

Note

Only users who are assigned the admin management role are permitted to access the system using FTP.

`adminaccess ftp del` *`host-list`*
Remove one or more hosts (IP addresses, hostnames, or asterisks) from the FTP list. Multiple entries may be separated by commas, spaces, or both. Role required: admin.

`adminaccess ftp option reset [session-timeout]`
Reset the FTP options to default values. Role required: admin.

`adminaccess ftp option set session-timeout` *`timeout-in-secs`*
Set the FTP client session timeout. Role required: admin.

`adminaccess ftp option show`
Show the current FTP options. Role required: admin, security, user, backup-operator, or none.

adminaccess ftps

`adminaccess ftps add` *`host-list`*
Add one or more hosts to the FTPS list. You can identify a host using a fully qualified hostname, an IPv4 address, or an IPv6 address. Host entries cannot include a space. Multiple entries may be separated by commas, spaces, or both. Role required: admin.

Note

Only users who are assigned the admin management role are permitted to access the system using FTPS.

`adminaccess ftps del` *`host-list`*
Remove one or more hosts (IP addresses, hostnames, or asterisk) from the FTPS list. Host entries may be separated by commas, spaces, or both. Role required: admin.

`adminaccess ftps option reset [session-timeout]`
Resets the FTPS options to default values. Role required: admin.

`adminaccess ftps option set session-timeout` *`timeout-in-secs`*
Sets the FTPS client session timeout. Role required: admin.

`adminaccess ftps option show`
Shows the current FTPS options. Role required: admin, security, user, backup-operator, or none.

adminaccess http

`adminaccess http add` *`host-list`*
Add one or more hosts to the HTTP/HTTPS list. You can identify a host using a fully qualified hostname, an IPv4 address, or an IPv6 address. Host entries cannot include a space. Multiple entries may be separated by commas, spaces, or both. Role required: admin.

`adminaccess http del` *`host-list`*
Remove one or more hosts (IP addresses, hostnames, or asterisk) from the HTTP/HTTPS list. Host entries may be separated by commas, spaces, or both. Role required: admin.

adminaccess reset

`adminaccess reset {http | https | ftp | ftps | telnet | ssh | scp | all}`
Reset one or more protocols to their default states and clear the access lists of host entries. Output shows the running state of each protocol. Role required: admin.

Note

Because SCP works together with SSH, output appears the same for both. However, due to the registry configuration, output could be misleading. For example, if SSH is disabled, SCP also shows as disabled; however, SCP is enabled at the registry level. This is expected behavior and does not affect functionality. When a user resets SCP, the SCP registry entry changes to enabled and output for SSH shows as enabled.

`adminaccess reset ssh-keys [user` *`username`*`]`

Remove the authorized SSH keys file for a user specified user or for the operator account from the Data Domain system. After removing the file, every SSH connection requires password authentication. Role required:

- Users may reset their own keys only.
- *Admin* role users may reset the keys of any user.
- *Security* role users and *none* role users may not reset keys.

adminaccess show

`adminaccess show`

List the access services available on a Data Domain system and display option values for the access services that are enabled. Role required: admin, security, user, backup-operator, or none.

- N/A means the service does not use an access list.
- A hyphen means the service can use an access list, but the access list does not contain host names.
- An asterisk means the service allows all hosts.

`adminaccess show ssh-keys [user` *`username`*`]`

Display the authorized SSH key file with a line number for each entry. *Admin* role users can view the SSH key files of any user. Users in other roles can view their own SSH key file only.

adminaccess ssh

`adminaccess ssh add` *`host-list`*

Add one or more hosts to the SSH list. You can identify a host using a fully qualified hostname, an IPv4 address, or an IPv6 address. Host entries cannot include a space. Multiple entries may be separated by commas, spaces, or both. Role required: admin.

`adminaccess ssh del` *`host-list`*

Remove one or more hosts (IP addresses, hostnames, or asterisks) from the SSH list. Host entries may be separated by commas, spaces, or both. Role required: admin.

`adminaccess ssh option reset [server-port | session-timeout]`

Reset the SSH options to default values. Role required: admin.

`adminaccess ssh option set server-port` *`port-number`*

Set the SSH server port. Role required: admin.

`adminaccess ssh option set session-timeout` *`timeout-in-secs`*

Set the SSH client timeout options. Role required: admin.

Example 2

Set the SSH session timeout period to 10 minutes:

```
# adminaccess ssh option set session-timeout 600
```

`adminaccess ssh option show`

Display the SSH options. Role required: admin.

adminaccess telnet

`adminaccess telnet add` *`host-list`*
Add one or more hosts to the Telnet list. You can identify a host using a fully qualified hostname, an IPv4 address, or an IPv6 address. Host entries cannot include a space. Multiple entries may be separated by commas, spaces, or both. Role required: admin.

`adminaccess telnet delete` *`host-list`*
Remove one or more hosts (IP addresses, hostnames, or asterisk) from the Telnet list. Host entries may be separated by commas, spaces, or both. Role required: admin.

`adminaccess telnet option reset [session-timeout]`
Reset the client session timeout period to the default value none to prevent client sessions from timing out. Role required: admin.

`adminaccess telnet option set session-timeout` *`timeout-in-secs`*
Set the client session timeout period to the specified number of seconds. If no data is received from a Telnet client within the timeout period, and if the client does not respond to a subsequent prompt message, the session terminates. The valid range is from 60 to 31536000 (365 days).

To configure the Data Domain system to prevent sessions from timing out, use the adminaccess telnet option reset command option. Role required: admin.

Example 3

To set the SSH session timeout period to 10 minutes:

```
# adminaccess telnet option set session-timeout 600
```

`adminaccess telnet option show`
Display the Telnet options. Role required: admin.

adminaccess trust

`adminaccess trust add host` *`hostname`* `[type mutual]`
Establishes the (mutual) trust with the specified host. Role required: admin.

`adminaccess trust copy {source | destination}` *`hostname`*
Copy all trust to or from the specified host. Role required: admin.

`adminaccess trust del host` *`hostname`* `[type mutual]`
Remove the mutual trust from the specified host. Role required: admin.

`adminaccess trust show [hostname]`
Show the list of trusted Certificate Authorities (CAs). Role required: admin, security, user, backup-operator, or none.

adminaccess web

`adminaccess web option reset [http-port | https-port | session timeout]`
Reset the Web options to default values. Role required: admin.

`adminaccess web option set http-port` *`port-number`*
Set the HTTP access port for the Web client. Default is port 80. Role required: admin.

`adminaccess web option set https-port` *`port-number`*
Set the HTTPS access port for the Web client. Default is port 443. Role required: admin.

`adminaccess web option set session-timeout` *`timeout-in-secs`*
Set the Web client session timeout. Range is 300 to 31536000 seconds; the default is 10800 seconds. Role required: admin.

`adminaccess web option show`
Show the current values for Web options. Role required: admin.

CHAPTER 2

alerts

The `alerts` command manages current alerts, alert notification groups, and alerts history. When a user logs in, a message is shown indicating the presence of alerts and instructions on how to proceed.

Command options enable sending email to a designated recipient or notification group when an event occurs within the Data Domain system. Depending on the option, information includes alert type, date posted, and resulting action. More than three months of alert history is retained.

The default alert notification group ("default") is configured to send alerts for any event class with severity level of Warning or above. Email notifications are sent to Data Domain Support at autosupport-alert@autosupport.datadomain.com. The default alert notification group can only be reset to default values: it cannot be destroyed.

Some event types, such as those in the environment class that pertain to temperature sensors within the chassis, are detected repeatedly if the underlying condition is not corrected.

This chapter contains the following topics:

alerts Change History

This section provides a list of changes since the 5.4 release, for all 5.5.x releases, in order of most recent release to first release.

Modified Arguments in DD OS 5.5

alerts show current [local]
The tenant-unit option is added:
alerts show current [local] [tenant-unit *tenant-unit*]

alerts show current-detailed [local] [alert-id *alert-id-list*]
The tenant-unit option is added:
alerts show current-detailed [local] [alert-id *alert-id-list* | tenant-unit *tenant-unit*]

alerts show history [local] [last *n* {hours | days | weeks | months}] [start *MMDDhhmm* [[*CC*] *YY*] end *MMDDhhmm* [[*CC*] *YY*]]
The tenant-unit option is added:
alerts show history [local] [last *n* {hours | days | weeks | months}] [start *MMDDhhmm* [[*CC*] *YY*] end *MMDDhhmm* [[*CC*] *YY*]] [tenant-unit *tenant-unit*]

alerts show history-detailed [local] [last *n* {hours | days | weeks | months}] [start *MMDDhhmm* [[*CC*] *YY*] end *MMDDhhmm* [[*CC*] *YY*]]
The tenant-unit option is added:
alerts show history-detailed [local] [last *n* {hours | days | weeks | months}] [start *MMDDhhmm* [[*CC*] *YY*] end *MMDDhhmm* [[*CC*] *YY*]] [tenant-unit *tenant-unit*]

Modified Output in DD OS 5.5

alerts show current [local]
The tenant-unit option is added, and the output can display the tenant unit when SMT is enabled.

alerts show current-detailed [local] [alert-id *alert-id-list*]
The tenant-unit option is added, and the output can display the tenant unit when SMT is enabled.

alerts show all [local]
The output can display the tenant unit when SMT is enabled.

alerts show daily [local]
The output can display the tenant unit when SMT is enabled.

alerts show history [local] [last *n* {hours | days | weeks | months}] [start *MMDDhhmm* [[*CC*] *YY*] end *MMDDhhmm* [[*CC*] *YY*]]
The tenant-unit option is added, and the output can display the tenant unit when SMT is enabled.

alerts show history-detailed [local] [last *n* {hours | days | weeks | months}] [start *MMDDhhmm* [[*CC*] *YY*] end *MMDDhhmm* [[*CC*] *YY*]]
The tenant-unit option is added, and the output can display the tenant unit when SMT is enabled.

Modified Behavior in DD OS 5.5

alerts notify-list test {group *group-name* | email *email-addr*}
This command can be executed by users with tenant-admin or tenant-user privileges

alerts clear

alerts clear alert-id *alert-id-list*
Clear an active alert or list of alerts. Role required: admin.

Argument Definitions

alert-id-list
List of alert identification numbers.

alerts notify-list

alerts notify-list add *group-name* { [class *class-list* [severity *severity*]] [emails *email-addr-list*] }
Modify a notification group by adding an event class, severity level, or recipient email address. Role required: admin, tenant-admin.

Example 4

```
# alerts notify-list add eng_lab emails mlee@urcompany.com,
bob@urcompany.com
```

alerts notify-list create *group-name* {class *class-list* [severity *severity*] | tenant-unit *tenant-unit*}
Subscribe to a notification list, add a class and a severity level to an existing list, or add members to a notification group on a Data Domain system or tenant unit. Role required: admin.

Example 5

```
# alerts notify-list create eng_grp class hardwareFailure
```

alerts notify-list del *group-name* { [class *class-list*] [emails *email-addr-list*]}
Modify an alert notification group by deleting event classes, email recipients, or both.

Security officer authorization is required only if the *group-name* has a severity level of Warning or above and the command is run on a Retention Lock Compliance system. See the *EMC Data Domain Operating System Administration Guide* for details on alerts. Role required: admin, tenant-admin.

Example 6

```
# alerts notify-list del eng_grp class hardwareFailure
```

alerts notify-list destroy *group-name*
Delete an alert notification group. Note that the default alert notification group cannot be destroyed.

Security officer authorization is required only if the *group-name* has a severity level of Warning or above and the command is run on a Retention Lock Compliance system. See the *EMC Data Domain Operating System Administration Guide* for details on alerts. Role required: admin.

`alerts notify-list reset`
Remove all user-created alert notification groups and restore the default notification group email list to factory defaults.

Role required: admin. Security officer authorization is required for systems with Retention Lock Compliance.

`alerts notify-list show [group` *`group-name`* `| email` *`email-addr`*`] | tenant-unit` *`tenant-unit`*`]`
Display the configuration of notification lists for groups or tenant units. Role required: admin, tenant-admin, security, user, tenant-user, backup-operator, or none.

Example 7

```
# alerts notify-list show eng_lab mlee@yourcompany.com
```

`alerts notify-list test {group` *`group-name`* `| email` *`email-addr`*`}`
Send a test notification to an alert notification group or email address. Role required: admin, tenant-admin, security, user, backup-operator, or none.

Example 8

```
# alerts notify-list test jsmith@yourcompany.com
```

Argument Definitions

class ***class-list***
(Optional) List of event classes: `cifs`, `cluster`, `environment`, `filesystem`, `firmware`, `hardwareFailure`, `network`, `replication`, `security`, `storage`, `syslog`, and `systemMaintenance`.

emails ***email-addr-list***
(Optional) Email addresses of members in an alert notification group.

group-name
Name of alert notification group.

severity ***severity***
(Optional) Severity level of event class: `alert`, `critical`, `debug`, `emergency`, `error`, `info`, `notice`, and `warning`. Default is `warning`.

tenant unit
The basic unit of a multi-tenancy configuration. A tenant unit is a secure, isolated partition for tenant-specific data and control flow within a Data Domain system. See the *EMC Data Domain Secure Multi-Tenancy User's Guide* for more information on SMT.

alerts show

`alerts show all [local]`
Display details on all alert notification groups. Role required: admin, security, user, backup-operator, or none.

`alerts show current [local] [tenant-unit` *`tenant-unit`*`]`

Display a list of currently active alerts on a Data Domain system or tenant unit. Role required: admin, tenant-admin, security, user, tenant-user, backup-operator, or none.

`alerts show current-detailed [local] [alert-id` *`alert-id-list`* `] [ tenant-unit` *`tenant-unit`*`]`

Display detailed information about currently active alerts on a Data Domain system or tenant unit. Role required: admin, tenant-admin, security, user, tenant-user, backup-operator, or none.

`alerts show daily [local]`

Display daily alert report, including current alerts and 24-hour alert history. Role required: admin, security, user, backup-operator, or none.

`alerts show history [local] [tenant-unit` *`tenant-unit`*`] [last` *`n`* `{hours | days | weeks | months}] [start` *`MMDDhhmm`* `[[`*`CC`*`]`*`YY`*`] end` *`MMDDhhmm`* `[[`*`CC`*`]`*`YY`*`]`

Display alert history on a Data Domain system or tenant unit. Default duration spans the last three months. Role required: admin, tenant-admin, security, user, tenant-user, backup-operator, or none.

`alerts show history-detailed [local] [tenant-unit` *`tenant-unit`*`] [last` *`n`* `{hours | days | weeks | months}] [start` *`MMDDhhmm`* `[[`*`CC`*`]`*`YY`*`] end` *`MMDDhhmm`* `[[`*`CC`*`]`*`YY`*`]`

Display detailed information about historic alerts on a Data Domain system or tenant unit. Default duration spans the last three months. Role required: admin, tenant-admin, security, user, tenant-user, backup-operator, or none.

Argument Definitions

alert-id-list
List of alert identification numbers.

last *n* {hours | days | weeks | months}
Use with show option to display alerts for most recent number of *n* (`hours`, `days`, `weeks`, `months`).

tenant-unit
The basic unit of a multi-tenancy configuration. A tenant unit is a secure, isolated partition for tenant-specific data and control flow within a Data Domain system. See the *EMC Data Domain Secure Multi-Tenancy User's Guide* for more information on SMT.

CHAPTER 3

alias

The `alias` command creates, deletes, and displays command aliases for the Data Domain system command set. Users can administer aliases only for commands for which they have permission.

This chapter contains the following topics:

alias Change History

There have been no changes to this command since the 5.4 release.

alias Guidelines and Restrictions

- A new alias is available only to the user who created it on the Data Domain system.

alias add

`alias add` *`alias-name`* "*`command`*"

Add a command alias. Enter the alias name and command, and enclose the command name in quotation marks. The new alias is available only to the user who created it. Role required: admin, security, user, backup-operator, or none.

Default Command Aliases

The following command aliases are included with the system and available to all users.

date
system show date

df
filesys show space

hostname
net show hostname

ifconfig
net config

iostat
system show stats

netstat
net show stats

nfsstat
nfs show stats

passwd
user change password

ping
net ping

poweroff
system poweroff

reboot
system reboot

sysstat
system show stats

traceroute
route trace

uname
system show version

uptime
: system show uptime

who
: user show active

alias del

`alias del` *`alias-name`*

Delete an alias by name. Role required: admin, security, user, backup-operator, or none.

alias reset

`alias reset`

Remove user-created aliases and restore defaults. Role required: admin, security, user, backup-operator, or none.

alias show

`alias show`

Display all aliases and command definitions. Role required: admin, security, user, backup-operator, or none.

CHAPTER 4

archive

The `archive` command is used only on systems licensed to run the EMC Data Domain Extended Retention software option (formerly Data Domain Archiver). Extended Retention command options enable the feature and configure policies. See the *EMC Data Domain Operating System Administration Guide* for details on functionality, installation, and configuration.

This chapter contains the following topics:

archive Change History

This section provides a list of changes since the 5.5 release, for all 5.6.x releases, in order of most recent release to first release.

Modified Arguments in DD OS 5.5.1

archive data-movement policy set age-threshold {*days* | never} mtrees *mtree-list*

Argument `days` must now be a minimum of 14 days.

archive data-movement policy set default-age-threshold {*days* | never}}

Argument `days` must now be a minimum of 14 days.

Modified Arguments in DD OS 5.5

archive data-movement schedule set {never | days *days* time *time* [every 2wks]} [no-clean]

New argument `[no-clean]` lets you skip file system cleaning after data movement.

archive report generate file-location [path {*path-list* | all}] [output-file *filename*]

New argument `[path {`*path-list*`| all}]` lets you specify a path or the entire namespace (all).

New argument `[output-file` *filename*`]` replaces former argument *filename*.

archive Guidelines and Restrictions

Supported configurations are:

- Controllers: DD860, DD990, DD4200, DD4500, DD7200.
- Storage expansion: EMC Data Domain ES20 expansion shelf and EMC Data Domain ES30 expansion shelf. A system may contain a mix of Data Domain ES20 and ES30 shelves; however, each shelf chain must contain ES20 shelves only or ES30 shelves only. Shelves within a chain cannot be mixed.

archive data-movement

`archive data-movement policy reset age-threshold mtrees` *`mtree-list`*

Reset the age threshold for specified MTrees (*mtree-list* is a colon-separated list). Only files modified in the past (beyond the age threshold) are moved to the retention tier during the next data movement. Role required: admin.

`archive data-movement policy reset default-age-threshold`

Reset the age threshold to the default value, which is set with `archive data-movement policy set default-age-threshold`.The default age threshold applies to new MTrees and to MTrees for which the age threshold has not been set. Role required: admin.

`archive data-movement policy set age-threshold {`*`days`*` | never} mtrees` *`mtree-list`*

Set the age threshold for specified MTrees (*mtree-list* is a colon-separated list). The value for *days* must be from 14 days to 18250 days (50 years). Role required: admin.

`archive data-movement policy set default-age-threshold {`*days*` | never}`
Set the default age threshold. The argument *days* must be from 14 days to 18250 days (50 years). Role required: admin.

`archive data-movement policy show [mtrees `*mtree-list*`]`
View the data-movement policy for the specified MTrees (*mtree-list* is a colon-separated list). Role required: admin.

`archive data-movement schedule reset`
Reset the data-movement schedule to default values. Role required: admin.

`archive data-movement schedule set {never | days `*days*` time `*time*` [every 2wks]} [no-clean]`
Set the schedule for data movement. Unless you specify `no-clean`, the file system is cleaned after data movement is completed. Note that the days argument checks two ranges (and can be either a space- or comma-separated list, or arbitrary text):

- Weekday (Monday-Sunday)
- Day of the month (1-31, regardless of month, plus “last” and “first”)

Any value outside of the two ranges generates an error message. Role required: admin.

Note

For days, “last” is converted to the value 31. If a schedule is set for the 31st of every month at 10:00 PM, it is not executed on months with fewer than 31 days. This is a known issue.

To schedule data movement to occur each Tuesday at 6:00 a.m., enter:

```
# archive data-movement schedule set days "tue" time "06:00"
```

To schedule data movement to occur on alternate Tuesdays at 6:00 a.m., enter:

```
# archive data-movement schedule set days "tue" time "06:00" every
2wks
```

`archive data-movement schedule show`
Display the data-movement schedule. Role required: admin, security, user, backup-operator.

`archive data-movement start`
Start data movement from the active tier to the retention tier. All files that satisfy the age-threshold value are moved to the retention tier. Data movement comprises five phases: seeding, scanning, verifying, packing, and installing. Role required: admin.

`archive data-movement status`
Display immediate, one-time view of output from the `archive data-movement start` command. Output shows the point at which data movement has progressed as of the time the command is issued. Role required: admin, security, user, backup-operator.

`archive data-movement stop`
Stop data movement to the retention tier. Role required: admin.

`archive data-movement throttle reset`
Resets the throttle value to 100 percent (no throttle). The throttle value will take effect without restarting file migration if it is running. Role required: admin.

`archive data-movement throttle set {25 | 50 | 75 | 100 }`
Sets the throttle value to 25, 50, 75, or 100, where 25 is the slowest, and 100 is the fastest. The throttle value will take effect without restarting file migration if it is running. Role required: admin.

`archive data-movement throttle show`
Shows the actual throttle value. Role required: admin.

`archive data-movement watch`
View data movement progress while the operation is running. If the operation has completed or is not running, output shows current status only. Role required: admin, security, user, backup-operator.

archive disable

`archive disable`
Disable the Extended Retention software option. Note that the file system must be destroyed (and all data lost) before Extended Retention can be disabled. Role required: admin.

archive enable

`archive enable`
Enable the Extended Retention software option. The file system must be disabled before Extended Retention can be enabled. Role required: admin.

Note

MTree replication is supported from Extended Retention systems to non-Extended Retention systems if both are running DD OS 5.5.

archive option

`archive option reset local-compression-type`
Reset the local compression algorithm to default value `gz` for subsequent data movement to the retention tier. You must restart the file system for the change to take effect. Role required: admin.

`archive option set local-compression-type {none | lz | gzfast | gz}`
Set the local compression algorithm for subsequent data movement to the retention tier. You must restart the file system for the change to take effect. Role required: admin.

`archive option show [local-compression-type | data-movement-packing]`
Display the local compression algorithm for the retention tier or the progress of the file migration process. Role required: With the exception of users assigned to the none management role, all users may run this command option.

archive report

`archive report generate file-location [path {`*`path-list`*` | all}] [output-file `*`filename`*`]`

Create a report showing the name and location of each file in a directory, an MTree, or the entire namespace. If the `output-file` *filename* argument is specified, the report is saved in this file under the fixed directory `/ddr/var`. If the output file argument is not specified, the report is displayed in the standard output. The command returns before the entire report is generated, and a footer indicates that the report is complete. Each line in the report contains a file name and its location. The location is shown as "Active" if the file completely resides in the active tier. If the file resides partially or completely in the retention tier, the retention unit name is shown for its location. An asterisk is appended to the line if the file contents span the active tier and retention unit. Role required: admin.

Examples

- To report files in a directory, use:

```
archive report generate file-location path /backup/dir1 output-
file report.txt
```

  or

```
archive report generate file-location path /data/col1/mtree-2/dir3
output-file report.txt
```

- To report files in an MTree, use:

```
archive report generate file-location path /data/col1/mtree-2
output-file report.txt
```

- To report files in the entire namespace, use:

```
archive report generate file-location path all output-file
report.txt
```

  or

```
archive report generate file-location output-file report.txt
```

archive show

`archive show config`

Display the Extended Retention configuration. Role required: With the exception of users assigned to the none management role, all users may run this command option.

Example 9

```
# archive show config
Enabled                                          Yes
Data movement Schedule                           No schedule
Default age threshold data movement policy       0 days
Run filesys clean after archive data movement    Yes
Retention Tier local compression                 gz
Packing data during archive data movement        enabled
Space Reclamation                                disabled
```

archive space-reclamation

`archive space-reclamation resume`

Resumes the retention tier space reclamation process. Role required: admin.

`archive space-reclamation start`

Starts the retention tier space reclamation process. The space reclamation process runs continuously until stopped or suspended explicitly, or preempted internally by a higher-

priority process, such as `archive data-movement` or `filesys clean`. Role required: admin.

`archive space-reclamation status`
Shows the status of the retention tier space reclamation process. Role required: admin.

Example 10

```
# archive space-reclamation status
Space-reclamation was started on March 9 2014 10:25 and is currently
running.
```

`archive space-reclamation status-detailed`
Shows the detailed status of the retention tier space reclamation process. Role required: admin.

`archive space-reclamation stop`
Stops the retention tier space reclamation process. Role required: admin.

`archive space-reclamation suspend`
Suspends the retention tier space reclamation process. Role required: admin.

CHAPTER 5

authentication

The `authentication` command manages NIS users, domains, groups and servers. Command options enable the Data Domain system to participate in an active Network Information Service (NIS) domain, which maintains a centralized repository of users, groups, and server names. NIS adds a global directory that authenticates users from any host on the network.

This chapter contains the following topics:

authentication Change History

This section provides a list of changes since the 5.4 release, for all 5.5.x releases, in order of most recent release to first release.

New Commands in DD OS 5.5.1

authentication kerberos keytab import
Imports krb5.keytab file from /ddr/var to /ddr/etc.

authentication kerberos reset
Resets the realm, KDC, etc. Unjoins the system from a UNIX KDC or Windows AD.

authentication kerberos set realm <home-realm> kdc-type {windows [kdcs <kdc-list>] | unix kdcs <kdc-list>}
Joins a DDR to Windows AD or Unix KDC.

authentication kerberos show config
Show Kerberos configuration.

Modified Output in DD OS 5.5

authentication nis groups show
The role column now displays SMT roles for the each group.

authentication nis show
This command now displays host names instead of IP addresses.

Modified Behavior in DD OS 5.5

authentication nis groups add *group-list* role {user | admin | backup-operator}
This command now displays an error if you try to add an existing tenant-user or tenant-admin group to the NIS group.

authentication kerberos

`authentication kerberos keytab import`
Imports the krb5.keytab file from /ddr/var to /ddr/etc. If the file is not present in /ddr/var, then the command returns an error. Role required: admin.

`authentication kerberos reset`
Resets the realm, KDC, and so on, to default configuration. Unjoins a DDR from the domain and unjoins a DDR from a Linux KDC and a Windows KDC. Role required: admin.

Note

To make a DDR part of Windows AD, first unjoin the DDR from the Linux KDC using this command.

`authentication kerberos set realm home-realm kdc-type {windows [kdcs kdc-list] | unix kdcs kdc-list}`
Sets the realm for a system and enables Kerberos authentication on the realm. Role required: admin.

Argument definitions

home-realm
The Kerberos realm.

kdc-type
Key Distribution Center type - Windows or UNIX.

kdc-list
List of KDCs.

`authentication kerberos show config`
Displays Kerberos configuration. Role required: admin.

Example 11

`authentication kerberos show config`

```
Home Realm:           abc.com
KDC List:             10.10.10.10 10.10.10.11
KDC Type:             windows
```

Output definitions

Home Realm
The Kerberos Realm.

KDC List
List of KDCs.

KDC Type
Key Distribution Center type - Windows or UNIX.

authentication nis

`authentication nis disable`
Disable the NIS client. Role required: admin.

`authentication nis domain reset`
Reset the NIS domain name. Role required: admin.

`authentication nis domain set` *`domain`* `[servers` *`server-list`*`]`
Set the NIS domain name and optionally add NIS servers to the *server-list*. Role required: admin.

`authentication nis domain show`
Display the NIS domain name. Role required: admin, security, user, backup-operator, or none.

`authentication nis enable`
Enable the NIS client. Role required: admin.

`authentication nis groups add` *`group-list`* `role {user | admin | backup-operator}`
Add a role-based access control (RBAC) role for NIS users in the *group-list*. You cannot add an existing tenant-admin group or tenant-user group to an NIS group. See the *EMC Data Domain Operating System Administration Guide* for role definitions. Role required: admin.

Example 12

Example 12 (continued)

```
# authentication nis groups add "tu1_user group1" role admin
**** "tu1_user group1" is currently an tenant-user group.
```

`authentication nis groups del` *`group-list`* `role {user | admin | backup-operator}`
Delete a role-based access control (RBAC) role for NIS users in the *group-list*. See the *EMC Data Domain Operating System Administration Guide* for role definitions. Role required: admin.

`authentication nis groups reset`
Delete all added NIS groups. Role required: admin.

`authentication nis groups show`
Display lists of NIS user groups and NIS admin groups. Role required: admin, security, user, backup-operator, or none.

Example 13

```
# authentication nis groups show
NIS Group   Role
---------   ------------------
group1      user, tenant-admin
group2      user, tenant-user
---------   ------------------
```

`authentication nis reset`
Delete the NIS configuration and set it to the default. Role required: admin.

`authentication nis servers add` *`server-list`*
Add NIS servers to the *server-list*. Role required: admin.

Note

If you add an invalid server name and enable NIS authentication, the system will continue to use the last valid server name, and it will display the YOUR DATA IS IN DANGER message in the system prompt. To correct this: enter `authentication nis servers reset`, `authentication nis domain reset`, and `authentication nis disable`; correct the server entries; and enter `authentication nis enable`.

`authentication nis servers del` *`server-list`*
Delete NIS servers from the *server-list*. Role required: admin.

`authentication nis servers reset`
Reset the NIS servers to their default settings. Role required: admin.

`authentication nis servers show`
Display a list of NIS servers. Role required: admin, security, user, backup-operator, or none.

`authentication nis show`
Display the NIS configuration. Role required: admin, security, user, backup-operator, or none.

`authentication nis status`
Display the NIS status. Role required: admin, security, user, backup-operator, or none.

CHAPTER 6

authorization

The `authorization` command, which is available only to security officers, establishes or modifies runtime authorization policy. Command options enable security-based functions such as managing filesystem encryption and enabling or disabling authorization policy.

All authorization tasks are logged automatically. The log file includes a timestamp, the identities of the security officer and administrative user, and the Data Domain system on which the task was performed. This log file serves as the audit trail, or "authorization history," for each action.

This chapter contains the following topics:

authorization Change History

There have been no changes to this command since the 5.4 release.

authorization Guidelines and Restrictions

- Procedures requiring authorization must be dual-authenticated by the security officer and the user in the admin role. For example, to set encryption, the admin enables the feature and the security officer enables runtime authorization.

authorization policy

`authorization policy reset security-officer`
Reset runtime authorization policy to defaults. Resetting authorization policy is not allowed on Retention Lock Compliance systems. Role required: security.

`authorization policy set security-officer {enabled | disabled}`
Enable and disable runtime authorization policy. Disabling authorization policy is not allowed on Retention Lock Compliance systems. Role required: security.

Example 14

```
# authorization policy set security-officer enabled
```

`authorization policy show`
Show the current authorization policy configuration. Role required: security.

authorization show

`authorization show history [last` *n* `{ hours | days | weeks }]`
View or audit past authorizations according to the interval specified. Role required: security.

CHAPTER 7

autosupport

The `autosupport` command manages system reports. Command options enable administrative users to manage two reports that describe the state of a Data Domain system: the `autosupport` report and the daily alert summary. By default, both reports are emailed to the Support address only, but users with admin role permissions may configure additional addresses and designate a subject tag keyword to bypass filtering that may block email delivery. For details on configuring `autosupport` notifications, see the *EMC Data Domain Initial Configuration Guide*.

This chapter contains the following topics:

autosupport Change History

There have been no changes to this command since the 5.4 release.

autosupport Guidelines and Restrictions

- Use the up and down arrow keys to move through the log. Use the q key to exit. Enter a forward slash and a pattern to search for dates.

autosupport add

`autosupport add {alert-summary | asup-detailed} emails` *`email-list`*

Add entries to the email list for the daily alert summary or the autosupport report. Role required: admin.

Example 15

```
# autosupport add asup-detailed emails djones@company.com
```

Argument Definitions

alert-summary
Addresses in email list for the Daily Alert Summary.

email-list
Individual email addresses to add to the specified list. Separate the items in the list with commas, spaces, or both.

autosupport del

`autosupport del {alert-summary | asup-detailed} emails` *`email-list`*

Delete entries from the email list for the daily alert summary or the autosupport report. Role required: admin.

Argument Definitions

alert-summary
Addresses in email list for the Daily Alert Summary.

email-list
Individual email addresses to add to the specified list. Separate the items in the list with commas, spaces, or both.

autosupport reset

`autosupport reset {alert-summary | asup-detailed}`

Reset asup-detailed email list or alert-summary email list to the default value. Role required: admin.

`autosupport reset all`

Reset all autosupport command options to the default values. Output includes details on where alert summaries are sent via email and alert summary schedules. Role required: admin.

`autosupport reset schedule [alert-summary | asup-detailed]`
Reset the schedules of the daily alert summary and the autosupport report to the default values.

- By default, the schedule for the daily alert summary is configured with the daily 0600 options.
- By default, the schedule for the autosupport report is configured with the daily 0800 options.

Role required: admin.

`autosupport reset subject-tag`
Reset subject tag to empty for the autosupport report and Daily Alert Summary. Role required: admin.

Argument Definitions

alert-summary
Addresses in email list for the Daily Alert Summary.

autosupport send

`autosupport send [email-addr] [cmd "cmd"]`
Email a report or command description to the autosupport report email list or to the address specified. You must enclose the command option name in double quotation marks. Role required: admin, security, user, backup-operator, or none.

Example 16

To run the net show stats command and email the results to djones@yourcompany.com:

```
# autosupport send djones@yourcompany.com cmd "net show stats"
```

Argument Definitions

“cmd”
Run the specified DD OS command. Enclose the command in double quotation marks.

email-list
Individual email addresses to add to the specified list. Separate the items in the list with commas, spaces, or both.

autosupport set

`autosupport set schedule {alert-summary | asup-detailed} {[{daily | day(s)} time] | never}`
Schedule the daily alert summary or the autosupport report. For either report, the most recently configured schedule overrides the previously configured schedule. Role required: admin.

Example 17

To schedule the daily alert summary for 2 p.m. Monday and Friday:

```
# autosupport set schedule alert-summary mon,fri 1400
```

Example 18

To schedule the autosupport report for Tuesday at 4 a.m:

```
# autosupport set schedule asup-detailed tue 0400
```

Example 19

To schedule the autosupport report for Tuesday at 3 p.m.:

```
# autosupport set schedule asup-detailed tue 1500
```

`autosupport set subject-tag` *tag*
Include the subject tag in the subject line of autosupport report and daily alert summary emails to filter the emails based on *tag*. This enables users to bypass filtering software that may block the emails. Default is none. Maximum number of characters is 64. Role required: admin.

Argument Definitions

alert-summary
Addresses in email list for the Daily Alert Summary.

daily
Default setting for daily alert summary and the autosupport report.

tag
A keyword that appends the subject line of the daily alert summary and autosupport report emails and enables users to bypass company filtering and avoid mis-routing.

autosupport show

`autosupport show {all | alert-summary | asup-detailed}`
Display the autosupport configuration. Role required: admin, security, user, backup-operator, or none.

Example 20

```
# autosupport show all
The Admin email is:
Detailed autosupport and alert summary to Data Domain currently
enabled.
Detailed autosupport is scheduled to run "daily" at "0600".
Detailed autosupport is sent to:
    myemail1@abc.com
    myemail2@abc.com
    autosupport@autosupport.datadomain.com

Alert summary is scheduled to run "daily" at "0800".
Alert summary is sent to:
    myemail1@abc.com
```

Example 20 (continued)

```
    myemail2@abc.com
    autosupport@autosupport.datadomain.com
```

`autosupport show history`
Display the event history file, which includes the date for each autosupport report. Message system logs are retained for 10 weeks. Role required: admin, security, user, backup-operator, or none.

`autosupport show report`
Generate an autosupport report without sending the results to the autosupport report email list. Role required: admin, security, user, backup-operator, or none.

`autosupport show schedule [alert-summary | asup-detailed]`
Display the schedules for the daily alert summary and the autosupport report. Role required: admin, security, user, backup-operator, or none.

`autosupport show support-list`
This command is deprecated. Role required: backup-operator.

`autosupport show support-notify`
Display the autosupport status (enabled or disabled) and the email destination. Role required: backup-operator.

`autosupport show subject-tag`
Show the subject tag for autosupport report and daily alert summary emails. Role required: admin.

Argument Definitions

alert-summary
Addresses in email list for the Daily Alert Summary.

tag
A keyword that appends the subject line of the daily alert summary and autosupport report emails and enables users to bypass company filtering and avoid mis-routing.

autosupport test

`autosupport test {alert-summary | asup-detailed | support-notify} | email` *`email-addr`*
Send a test email to all lists, or to a specific address. Role required: admin, security, user, backup-operator, or none.

Argument Definitions

alert-summary
Addresses in email list for the Daily Alert Summary.

email-list
Individual email addresses to add to the specified list. Separate the items in the list with commas, spaces, or both.

CHAPTER 8

cifs

The `cifs` command manages CIFS data access between a Data Domain system and Windows clients. Command options enable and disable access to a Data Domain system from media servers and other Windows clients that use the CIFS protocol. The `cifs` command sets the authentication mode, share management, and administrative access, and displays status and statistics for CIFS clients.

This chapter contains the following topics:

cifs Change History

This section provides a list of changes since the 5.4 release, for all 5.5.x releases, in order of the most recent release to the first release.

Modified Output in DD OS 5.5.1

cifs set authentication active-directory
The output now conveys that NFS clients will be able to use Kerberos authentication.

New Commands in DD OS 5.5

cifs local-group commands
Add and delete a domain user or domain group to the CIFS local group or display information about a cifs local group.

cifs option reset f5
Reset a cifs option to the default value.

cifs option reset server signing
Resets server signing to disabled, which is the default.

cifs option set f5
Sets a cifs option for Data Domain systems using F5 Network's tiered storage solution ARX.

cifs option set server signing
Enable Server Message Block (SMB) signing, a security mechanism that improves the security of the SMB protocol.

Modified Output in DD OS 5.5

cifs show active
Output now displays information by column: Computer, User, Open Files, Connect Time (sec), Idle Time (sec). The Open Files information is displayed by column too: User, Mode, Locks, File. A summary of total sessions and total open files is also displayed.

Deprecated Commands in DD OS 5.5

cifs add /backup *client-list*
An alternative command is `cifs share create backup path /backup clients` *client-list*, if applicable.

cifs add /ddvar *client-list*
An alternative command is `cifs share create ddvar path /ddvar clients` *client-list*, if applicable.

cifs del /backup *client-list*
An alternative command is `cifs share destroy backup`, if applicable.

cifs del /ddvar *client-list*
An alternative command is `cifs share destroy ddvar`, if applicable.

cifs hosts add *ipadd host-list*
(No alternative.)

cifs hosts del *ipaddr*
(No alternative.)

cifs hosts reset
(No alternative.)

cifs hosts show
(No alternative.)

cifs nb-lookup *netbios-name*
(No alternative.)

cifs reset clients
An alternative command is `cifs share destroy`, if applicable.

cifs reset wins-server
(No alternative.)

cifs set wins-server ipaddr
(No alternative.)

cifs show clients
An alternative command is `cifs share show`, if applicable.

cifs Guidelines and Restrictions

- After a CIFS client name has been added, it must be configured for access to the Data Domain system. Configuration instructions are provided in the Integration Documentation available through EMC online support at http://support.emc.com.
- When adding or removing clients on the Data Domain system `/backup` directory separate clients in the list by a comma, a space, or both. The client-list can contain class-C IP addresses, IP addresses with either netmasks or length, an IPv6 address, hostnames, or an asterisk followed by a domain name.
- Enter an asterisk to add or remove all clients on the network.
- CIFS must be enabled on the Data Domain system. See cifs enable on page 66.

cifs add

`cifs add /backup client-list`
Specify clients that can access a Data Domain system `/backup` directory. The `/backup` directory is the target directory for compressed backup server data. Role required: admin-role.

Note

This command is deprecated. An alternative command is `cifs share create backup path /backup clients client-list`

Note

If adding multiple clients, Data Domain recommends using the cifs share add command instead.

`cifs add /ddvar client-list`
Specify clients that can access a Data Domain system `/ddvar` directory. The `/ddvar` directory contains Data Domain system core and log files. Role required: admin-role.

Note

This command is deprecated. An alternative command is `cifs share create ddvar path /ddvar clients client-list`

cifs del

`cifs del /backup client-list`
Remove clients from the list of CIFS backup clients that can access a Data Domain system `/backup` directory. Role required: admin-role.

Note

This command is deprecated. An alternative command is `cifs share destroy backup`

Note

If removing multiple clients, Data Domain recommends using the cifs share destroy command instead.

`cifs del /ddvar client-list`
Remove one or more clients from the list of clients that can access a Data Domain system /ddvar directory. Role required: admin-role.

Note

This command is deprecated. An alternative command is `cifs share destroy ddvar`

cifs disable

`cifs disable`
Disable the CIFS service and prevent CIFS clients from connecting to the Data Domain system. This command option stops the CIFS file service only. CIFS authentication services continue to run. Role required: admin-role.

cifs enable

`cifs enable`
Enable the CIFS service and allow CIFS clients to connect to the Data Domain system. This command option starts the CIFS file service only. Role required: admin.

cifs hosts

`cifs hosts add ipaddrhost-list`
Add lmhosts mapping. The `lmhosts` file is a local text file that maps IP addresses to NetBIOS names. A single IP address can contain multiple hostnames. Role required: admin.

Note

This command is deprecated.

`cifs hosts del ipaddr`
Remove lmhosts mapping for the specified IP address. Role required: admin.

Note

This command is deprecated.

`cifs hosts reset`
Reset lmhosts mapping to the default. This option removes all IP address and NetBIOS hostnames from the `lmhosts` file. Role required: admin.

Note

This command is deprecated.

`cifs hosts show`
Display lmhosts mappings. Role required: admin, user, none.

Note

This command is deprecated.

cifs local-group

`cifs local-group add group-name members member-list`
Add a domain user or domain group to the cifs local group using a comma separated list. Role required: admin-role.

Note

Do not use
`cifs local-group add`
when an f5 option has already been set using the
`cifs option set f5`
command.

`cifs local-group del group-name members {all | member-list}`
Delete a domain user or domain group from the cifs local group using the word all or a comma separated list. Role required: admin.

`cifs local-group show list [group-name]`
Display brief information about the cifs local group, for example: group name and number of members present in this group. Role required: admin.

`cifs local-group show detailed [group-name]`
Display detailed information about the cifs local group, for example: group name, group SID (security identifier), and group ID as well as the group member names and their SIDs. Role required: admin.

cifs nb-lookup

`cifs nb-lookup netbios-name`
Display the IP address for the specified NetBIOS name. Role required: admin, user, backup-operator, security, none.

Note

This command is deprecated.

cifs option

`cifs option reset` *name*
Reset a CIFS option to default value. Role required: admin, user.

`cifs option reset f5` *name*
Reset a CIFS option to default value. For use with Data Domain Systems using F5 Network's tiered storage solution ARX. Role required: admin.

`cifs option set` *name value*
Set a CIFS option. Role required: admin, user.

`cifs option set f5` *name value*
Set a CIFS option. For use with Data Domain Systems using F5 Network's tiered storage solution ARX. Role required: admin.

Note

Do not use
`cifs option set f5`
when a CIFS local group has been set using the
`cifs local-group add`
command.

`cifs option show`
Display CIFS options. Role required: admin.

`cifs option reset server signing`
Resets server signing to disabled, which is the default. Role required: admin.

`cifs option set server signing [auto | mandatory]`
Server Message Block (SMB) signing is a security mechanism that improves the security of the SMB protocol. When enabled using the auto option, it is possible for clients that support SMB signing to connect, although it is also possible for clients that do not support SMB signing to connect. When SMB signing is enabled using the mandatory option, both computers in the SMB connection must support SMB signing, and the SMB connection will not be successful if one computer does not support SMB signing. Role required: admin.

cifs reset

`cifs reset authentication`
Reset the CIFS authentication to the default: workgroup. Role required: admin.

`cifs reset clients`
Reset the CIFS client access list for `/backup` and / ddvar shares to the default: no client access. Role required: admin.

Note

This command is deprecated. An alternative command is
`cifs share destroy`

`cifs reset nb-hostname`
Reset the NetBIOS hostname to the default: none. Role required: admin.

`cifs reset stats`

Reset cifs statistics. Role required: admin.

`cifs reset wins-server`
Set the WINS server IP address to the default: none. Role required: admin.

Note

This command is deprecated.

cifs set

`cifs set authentication active-directory` *realm* `{ [`*dc1* `[`*dc2* `...]] | * }`
Set authentication to Active Directory (AD). The realm must be a fully qualified name. Use commas, spaces, or both to separate entries in the domain controller list. Security officer authorization is required for systems with Retention Lock Compliance enabled. Role required: admin.

Note

Data Domain recommends using the asterisk to set all controllers instead of entering them individually.

Argument definitions

realm
The Windows Active Directory realm.

dc1, dc2
Domain Controller 1, Domain Controller 2.

When prompted, enter a name for a user account. The type and format of the name depend on if the user is inside or outside the company domain.

- For user “Administrator” inside the company domain, enter the name only: administrator.
- For user “Jane Doe” in a trusted domain, enter the user name and domain: jane.doe@trusteddomain.com. The account in the trusted domain must have permission to join the Data Domain system to your company domain.

The Data Domain system automatically adds a host entry to the DNS server. It is not necessary to create the entry manually.

If you set the NetBIOS hostname using the command `cifs set nb-hostname`, the entry is created for NetBIOS hostname only, not the system hostname. Otherwise, the system hostname is used.

`cifs set authentication workgroup` *workgroup*
Set the authentication mode to workgroup for the specified workgroup name. Role required: admin.

Argument definitions

workgroup
Workgroup name.

`cifs set nb-hostname` *nb-hostname*
Set the NetBIOS hostname. Role required: admin.

`cifs set wins-server` *ipaddr*

Set the WINS server IP address. If CIFS clients are using NetBIOS, a WINS server may be required to resolve NetBIOS names to IP addresses. Role required: admin.

Note

This command is deprecated.

cifs share

`cifs share create` *share* `path` *path* `{max-connections` *max connections* `| clients` *clients* `| browsing {enabled | disabled} | writable {enabled | disabled} | users` *users* `| comment` *comment*`}`

Create a new share. Role required: admin.

Argument Definitions

share
A descriptive name for the share.

path
The path to the target directory.

max-connections
The maximum number of connections to the share allowed at one time.

clients
A comma-separated list of clients allowed to access the share. Specify the clients by hostname or IP address. No spaces or tabs are allowed and the list must be enclosed in double quotes. If the clients argument is not specified when creating the share, the share is not accessible by any client. To make the share accessible for all clients, enter the clients argument and precede client name by an ampersand.

users
A comma-separated list of user names. Other than the comma delimiter, spaces (blank or tab) are treated as part of the user name because a Windows user name can have a space in the name.

The user names list can include group names. Group names must be preceded by the symbol for the word *at* (@).

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. Separate group and user names by commas only. Spaces may be included within a group name but are not allowed as delimiters for group names.

comment
A descriptive comment about the share.

`cifs share destroy` *share*

Delete a share. Role required: admin.

`cifs share disable` *share*

Disable a share. Role required: admin.

`cifs share enable` *share*

Enable a share. Role required: admin.

`cifs share modify` *share* `{max-connections` *max connections* `| clients` *clients* `| browsing {enabled | disabled} | writeable {enabled | disabled} | users` *users* `| comment` *comment*`}`

Modify a share configuration with the same configuration options as the cifs share create option, except for its path. You cannot change the path for an existing share. Modifications apply to new connections only. Role required: admin.

See the share create command option for a description of the command variables. To remove a user list for the share, specify *users*.

`cifs share show [share]`
Display share configurations for all shares, or for a specified or custom share. Role required: admin, user, backup-operator, security, none.

cifs show

`cifs show active`
Display all active CIFS clients. Role required: admin, user, backup-operator, security, none.

`cifs show clients`
Display all allowed CIFS clients for the default /ddvar administrative share and the default `/backup` data share. Role required: admin, user, backup-operator, security, none.

Note

This command is deprecated. An alternative command is `cifs share show`

`cifs show config`
Display the CIFS configuration. Role required: admin, user, backup-operator, security, none.

Note

In the command output, "Max open files per connection" displays the maximum number of open files on a Data Domain system, not the number of open files per connection.

`cifs show detailed-stats`
Display detailed statistics on CIFS activity and performance. Role required: admin, user, backup-operator, security, none.

`cifs show stats`
Display basic statistics on CIFS activity and performance. Role required: admin, user, backup-operator, security, none.

cifs status

`cifs status`
Show status of CIFS: enabled or disabled. Role required: admin, user, backup-operator, security, none.

cifs troubleshooting

`cifs troubleshooting domaininfo`
Report domain information; for example, to check the connectivity between the Data Domain system and the domain. Also to confirm if authentication issues are due to domain connectivity. Role required: admin.

`cifs troubleshooting group` *groupname* | *gid* | *SID*
List details for a specified group. Role required: admin.

`cifs troubleshooting list-groups`
List all CIFS groups. Role required: admin.

`cifs troubleshooting list-users`
List all CIFS users. Role required: admin.

`cifs troubleshooting performance`
Collect tcpdump and ddfs traces for CIFS performance analysis. Role required: admin.

Example 21

To troubleshoot performance problems:

Enter: **`cifs troubleshooting performance`**

Enter: **`support bundle upload`**

`cifs troubleshooting user` *username* | *uid* | *SID*
Display details on a specified user.

CHAPTER 9

config

The `config` command manages Data Domain system configuration settings. Command options include changing individual configuration parameters and viewing the configuration setup. For information on how to configure the system, see the *EMC Data Domain Operating System Initial Configuration Guide* and the *EMC Data Domain Operating System Administration Guide*.

This chapter contains the following topics:

config Change History

There have been no changes to this command since the 5.4 release.

config reset

`config reset location`
Reset the location description to the default Null. Role required: admin.

`config reset mailserver`
Reset the mail server to the default mail server. Role required: admin.

`config reset timezone`
Reset the time zone to the default US/Pacific. Role required: admin. This command option requires security officer authorization if Retention Lock Compliance is enabled on any MTrees.

config set

`config set admin-email` *`email-addr`*
Set the email address for the administrator who should receive system alerts and autosupport reports. The system requires one administrative email address. Use the `autosupport` and `alerts` commands to add other email addresses. To check the current setting, use `config show admin-email`. Role required: admin.

`config set admin-host` *`host`*
Set the machine from which you can log in to the Data Domain system to view system logs and use system commands. The hostname can be a simple or fully qualified hostname or an IP address. The specified host is also added to the FTP and Telnet lists configured with the `adminaccess` command and to the CIFS and NFS lists created with the `cifs share create` and `nfs add` commands. This command provides a quick way to add authentication privileges to multiple lists. To check the current setting, use `config show admin-host`. Role required: admin.

Example 22

```
# config set admin-host admin12.yourcompany.com
```

`config set location "`*`location`*`"`
Configure a description of a Data Domain system's location. A description of a physical location helps identify the machine when viewing alerts and autosupport emails. If the description contains one or more spaces, the description must be in double quotation marks. To check the current setting, use `config show location`. Role required: admin.

Example 23

```
# config set location "row2-num4-room221"
```

`config set mailserver` *`host`*

Configure the SMTP mail server used by the Data Domain system. To check the current setting, use `config show mailserver`. Role required: admin.

Example 24

```
# config set mailserver mail.yourcompany.com
```

`config set timezone` *zonename*

Set the system clock to a specific time zone. The default setting is US/Pacific. Do any of the following to see the time zone name options.

- Enter `config set timezone ?` to display a list of regional zone names.
- Enter `config set timezone` *region_zonename* to display zone names for cities and areas in the specified region.
- Enter `config set timezone etc` to display valid GMT zone names.
- See Appendix A in the *EMC Data Domain Operating System Command Reference*.

Note

For additional time zone names that are not displayed in DD OS, see the "Miscellaneous" section of Appendix A in the *EMC Data Domain Operating System Command Reference*.

Changes to the time zone require a system reboot. Role required: admin. This command option requires security officer authorization if any MTrees are enabled with Retention Lock Compliance.

config setup

`config setup`

Change configuration settings for the system, network, filesystem, CIFS, NFS, and licenses. Press Enter to cycle through the selections. You will be prompted to confirm any changes. Choices include **Save**, **Cancel**, and **Retry.**

This command option is unavailable on Retention Lock Compliance systems. Use System Manager to change configuration settings. Role required: admin.

config show

`config show admin-email`

Display the administrative email address the Data Domain system uses for email from the alerts and autosupport commands. Role required: admin, security, user, backup-operator, or none.

`config show admin-host`

Display the administrative host from which you can log into the Data Domain system to view system logs and use system commands. Role required: admin, security, user, backup-operator, or none.

`config show all`

Display all config command settings. Role required: admin, security, user, backup-operator, or none.

`config show location`

Display the Data Domain system location description, if you set one. Role required: admin, security, user, backup-operator, or none.

`config show mailserver`

Display the name of the mail server that the Data Domain system uses to send email. Role required: admin, security, user, backup-operator, or none.

`config show timezone`

Display the time zone used by the system clock. Role required: admin, security, user, backup-operator, or none.

CHAPTER 10

ddboost

The `ddboost` command manages the integration of Data Domain systems and disk backup devices. Command options create and delete storage units on the storage server, and display the disk space usage of each storage unit. The EMC Data Domain Boost software option also supports advanced load balancing and failover, distributed segment processing, encryption, and low-bandwidth optimization.

Quotas provision Data Domain system storage among different backup applications. Quotas restrict the logical (uncompressed and undeduplicated) storage capacity for each storage unit. DD Boost storage unit quota limits (hard or soft) can be set or removed dynamically. Quotas may also be used to provision various DD Boost storage units with different sizes, enabling an administrative user to monitor the usage of a particular storage unit over time. Note that it is possible to configure quotas on a system and run out of storage before quota limits are reached.

Like MTree quota limits, the `ddboost storage-unit create` command includes optional arguments to specify quota limits at the time the storage unit is created. Output of the `ddboost storage-unit show` command indicates if a quota is defined for the storage unit.

Fibre Channel transport is available for DD Boost via the DD Boost over Fibre Channel service and Automatic Image Replication (AIR) is also supported.

The Multiuser Storage Unit Access Control feature enhances the user experience by supporting multiple usernames for the DD Boost protocol, providing data isolation for multiple users sharing a Data Domain system. Using the DD Boost protocol, the backup application connects to the Data Domain system with a username and password to support this feature. Both the username and password are encrypted using public key exchange. The `tenant-unit` keyword is introduced to the `ddboost storage-unit` command for integration with the Secure Multi-Tenancy feature. One storage unit must be configured for each tenant unit. Each tenant unit can be associated with multiple storage units.

See the *EMC Data Domain Boost for OpenStorage Administration Guide* and the *EMC Data Domain Operating System Administration Guide* for details.

This chapter contains the following topics:

ddboost Change History

This section provides a list of changes since the 5.4 release, for all 5.5.x releases, in order of the most recent release to the first release.

New Commands in DD OS 5.5.2

ddboost storage-unit rename *storage-unit new-storage-unit*
Renames a storage unit.

ddboost storage-unit undelete *storage-unit*
Recovers a deleted storage unit.

Modified Arguments in DD OS 5.5.2

ddboost ifgroup add *group_name* {interface {*ipaddr* | *ipv6addr*} | client *host*}
Added the *ipv6addr* variable.

ddboost ifgroup del *group_name* {interface {*ipaddr* | *ipv6addr*} | client *host*}
Added the *ipv6addr* variable.

ddboost storage-unit create
Added the `report-physical-size` argument.

ddboost storage-unit modify
Added the `report-physical-size` argument.

Modified Behavior in DD OS 5.5.2

ddboost storage-unit delete *storage-unit*
The deleted storage-unit retains its old name and is shown as deleted in the mtree list.

New Command in DD OS 5.5.1

ddboost clients show active
Show DD Boost client activity.

New Commands in DD OS 5.5

ddboost clients add
Add clients to DD Boost client list.

ddboost clients del
Delete clients from DD Boost client list.

ddboost clients modify
Modify clients on the DD Boost client list.

ddboost clients reset
Reset DD Boost client list to factory default.

ddboost clients show config
Show DD Boost client list.

ddboost streams show active
Show active streams per `storage-unit`.

ddboost streams show history
Show streams history per `storage-unit`.

ddboost user assign
Assign user to DD Boost users list.

ddboost user option reset
Unassign DD Boost user from the default `tenant-unit`.

ddboost user option set
DD Boost user set a default `tenant-unit`.

ddboost user show
Show users in the DD Boost users list.

ddboost user unassign
Unassign user from the DD Boost users list.

Modified Arguments in DD OS 5.5

ddboost event show [all | storage-unit *local-storage-unit*
Added the `all` and `storage-unit` arguments, and *local-storage-unit* variable.

ddboost file-replication option reset
Added the `ipversion` argument.

ddboost file-replication option set
Added the `ipversion` argument, which can be set to `ipv4` or `ipv6`.

ddboost file-replication option show
Added the `ipversion` argument.

ddboost show connections
Added the optional `detailed` argument.

ddboost storage-unit create
Added these arguments: `user`, `tenant-unit`, `write-stream-soft-limit`, `read-stream-soft-limit`, `repl-stream-soft-limit`, and `combined-stream-soft-limit`.

ddboost storage-unit modify
Added these arguments: `user`, `tenant-unit`, `write-streamsoft-limit`, `read-stream-soft-limit`, `repl-stream-soft-limit`, and `combined-stream-soft-limit`.

Deprecated Commands in DD OS 5.5

ddboost access add clients *user-name*
Use `ddboost clients add` instead.

ddboost access del clients *user-name*
Use `ddboost clients del` instead.

ddboost access reset *user-name*
Use `ddboost clients reset` instead.

ddboost access show *user-name*
Use `ddboost clients show config` instead.

ddboost reset user-name *user-name*
Use `ddboost user unassign` instead.

ddboost set user-name *user-name*
Use `ddboost user assign` instead.

ddboost show user-name
Use `ddboost user show` instead.

Deleted Command in DD OS 5.5

`ddboost user del`

ddboost Guidelines and Restrictions

- DD Boost is a licensed software option. If basic options do not work, verify that the proper licensing has been implemented on your Data Domain system.
- Quota limits are enforced only if MTree quotas are enabled. A message displays in the output notifying users if the quota feature is disabled.
- When a storage unit is created, quota limits are set to the default MTree quota size.
- If MTree quotas are enabled, backups are stopped if a hard limit is reached.
- Enabling quotas may cause OpenStorage backup applications to report non-intuitive sizes and capacities. See Knowledge Base article 85210, available on the Support portal, for details.
- Only one Automatic Image Replication (AIR) association is allowed for a specified storage unit and the target Data Domain system and the target storage unit.
- Do not use DD Boost Fibre Channel server names to create AIR associations. Use IP server names only.

ddboost access

`ddboost access add clients` *`client-list`*

Add one or more clients to the list of clients that can access DD Boost. Enter the client hostname, not IP address.

Note

This command is deprecated. Use the `ddboost clients add` command instead.

Role required: admin.

Example 25

```
# ddboost access add clients host1 host2 host3
```

`ddboost access del clients` *`client-list`*

Remove one or more clients from the list of clients that can access DD Boost.

Role required: admin.

Note

This command is deprecated. Use the `ddboost clients del` command instead.

`ddboost access reset`

Reset DD Boost client list to factory default.

Note

This command is deprecated. Use the `ddboost clients reset` command instead.

Role required: admin.

`ddboost access show`

Show list of clients that can access DD Boost.

Note

This command is deprecated. Use the `ddboost clients show` command instead.

Role required: admin, security, user, backup-operator, none.

ddboost association

`ddboost association create` *`storage-unit`* `{replicate-to | replicate-from}` *`remote-hostname remote-storage-unit`*
Create a storage unit association for the specified storage unit, the target Data Domain system, and the target storage unit.

Role required: admin.

Example 26

```
# ddboost association create feature2 replicate-to kuma-ost11.emc.com feature2
DDBoost association created.
```

`ddboost association destroy` *`storage-unit`* `{replicate-to | replicate-from}` *`remote-hostname remote-storage-unit`*
Destroy the storage unit association of the specified storage unit, the target Data Domain system, and target storage unit.

Role required: admin.

Note

This command option deletes unprocessed events in the local storage unit if the association specified is {replicate-from}. It does not delete user data in the local storage unit.

`ddboost association show [all | storage-unit` *`storage-unit`*`]`
Show the storage unit association list for a specified local storage unit or all local storage units with an association.

Role required: admin, security, user, backup-operator, none.

ddboost clients

`ddboost clients add` *`client-list`* `[encryption-strength {medium| high}`
Add clients to DD Boost client list.

Role required: admin.

`ddboost clients del` *`client-list`*
Delete clients from DD Boost client list.

Role required: admin.

`ddboost clients modify` *`client-list`* `encryption-strength {none | {medium|high}`
Modify clients on the DD Boost client list.

Role required: admin.

`ddboost clients reset`
Reset DD Boost client list to factory default.

Role required: admin.

`ddboost clients show active [all | client` *`hostname`* `| storage-unit` *`storage-unit`* `| tenant-unit` *`tenant-unit`*`]`
Show DD Boost client activity. Information displayed includes interface used, operation (`read` or `write`), and mode. For read operations, mode can be `compressed`. For write operations, mode can be `dsp` and/or `synthetic`.

Role required: admin, tenant-admin, security, user, tenant-user, backup-operator, or none.

`ddboost clients show config`
Show DD Boost client list.

Role required: admin, security, user, backup-operator, none.

Example 27

```
# ddboost clients show config

Client                          Encryption Strength
-----------------------------   -------------------

*                               none
*.corp.emc.com                  medium
rtp-ost-ms02.emc.com            high
jsmith-dl.emc.com               high
```

ddboost destroy

`ddboost destroy`
Delete all storage units from the Data Domain system. The command permanently removes all data (files) contained in the storage units. You must also manually remove (expire) corresponding catalog entries in the backup software.

Role required: admin.

ddboost disable

`ddboost disable`
Disable DD Boost. During the process of disabling DD Boost, all file replication transfers and read/write jobs are also disabled.

Role required: admin, security.

ddboost enable

`ddboost enable`
Enable DD Boost. If the user, user ID (UID), or group ID (GID) changes, the Data Domain system updates all files and storage units the next time this command is run.

Role required: admin.

ddboost event

`ddboost event show [all | storage-unit` *`storage-unit`*`]`
Show the event list for the specified local storage unit or all local storage units with a {replicate-from} association.

Events formatted with the suffix `.event.nnnnnnn` have been processed but not yet deleted. Events formatted with the suffix `.imgset` have not yet been processed.

Role required: admin, security, user, backup-operator, none.

Example 28

```
# ddboost event show
DDBoost events:
test2:    bluemedia.emc.com_31234_6589_1.event.0000000000000006
192:rtp-ost-sparc1.emc.com_rtp-ost-dd670c2.emc.com_1328637954_1.imgset
```

Output Definitions (event.nnnnnnn)

first media server
Hostname of the media server to which the event is first delivered. In the example: bluemedia.emc.com.

proc_id
Process identifier on the first media server to which the event is initially delivered. In the example: 31234.

thread_id
Thread identifier on the first media server to which the event is first delivered. In the example: 6589.

 # images
Number of images contained in event. In the example: 1. Typically this number is 1 because only the IM image file is contained in an event.

event
Image set identifier. In the example: 0000000000000006.

Output Definitions (imgset)

job #
NetBackup duplication job identifier. In the example: 192.

source server
Hostname of the NetBackup server. In the example: rtp-ost-sparc1.emc.com.

source Data Domain system
Hostname of the Data Domain system from where event originated. In the example: rtp-ost-dd670c2.emc.com.

image date
NetBackup image time stamp. In the example: 1328637954.

 # images
Number of images contained in event. In the example: 1. Typically this number is 1 because only the IM image file is contained in an event.

imgset
Image set identifier.

ddboost fc

`ddboost fc dfc-server-name reset`
Reset DD Boost Fibre Channel server name.

Role required: admin.

`ddboost fc dfc-server-name set` *`server-name`*
Set DD Boost Fibre Channel server name. The default dfc-server-name is the Data Domain system hostname.

Role required: admin.

`ddboost fc dfc-server-name show`
Show DD Boost Fibre Channel server name.

Role required: admin, security, user, backup-operator, none.

`ddboost fc dump start logfile-id` *`logfile-id`* `[formatted] [snaplen` *`bytes`*`] [logfile-count-limit` *`count`*`] [logfile-size-limit` *`bytes`*`] [virtual-connection` *`virtual-connection-id`*`] [client-hostname` *`hostname`*`] [initiator` *`initiator`*`] [target-endpoint` *`endpoint`*`] [destination-tcp-port` *`tcp-port`*`]`
Start DD Boost Fibre Channel message tracing.

Role required: admin.

`ddboost fc dump status`
Show DD Boost Fibre Channel message tracing.

Role required: admin, security, user, backup-operator, none.

`ddboost fc dump stop`
Stop DD Boost Fibre Channel message tracing.

Role required: admin.

`ddboost fc group add` *`group-name`* `initiator` *`initiator-spec`*
Add one or more initiators to a DD Boost Fibre Channel group.

Role required: admin.

`ddboost fc group add` *`group-name`* `device-set [count` *`count`*`] [endpoint {all | none |` *`endpoint-list`*`}]`
Add one or more DD Boost devices to a DD Boost Fibre Channel group. Valid range for count argument is 1-64.

Role required: admin.

`ddboost fc group create` *`group-name`*
Create a DD Boost Fibre Channel group.

Role required: admin.

`ddboost fc group del` *`group-name`* `initiator` *`initiator-spec`*
Remove one or more initiators from a DD Boost Fibre Channel group.

Role required: admin.

`ddboost fc group del` *`group-name`* `device-set {count` *`count`* `| all }`
Remove one or more DD Boost devices from a DD Boost Fibre Channel group.

Role required: admin.

`ddboost fc group destroy` *`group-name`*
Destroy a DD Boost Fibre Channel group.

Role required: admin.

`ddboost fc group modify` *`group-name`* `device-set [count` *`count`*`] [endpoint {all | none |` *`endpoint-list`*`]`
Modify a device set for a DD Boost Fibre Channel group.

Role required: admin.

`ddboost fc group rename` *`src-group-name dst-group-name`*
Rename a DD Boost Fibre Channel group.

Role required: admin.

`ddboost fc group show detailed` *`group-spec`* `[initiator` *`initiator-name`*`]`
Show details of DD Boost Fibre Channel groups. Output includes information on device names, system addresses, LUNs, and endpoints.

Role required: admin, security, user, backup-operator, none.

`ddboost fc group show list [`*`group-spec`*`] [initiator` *`initiator-name`*`]`
Display a list of configured DD Boost Fibre Channel groups.

Role required: admin, security, user, backup-operator, none.

`ddboost fc show detailed-stats`
Show DD Boost Fibre Channel detailed statistics.

Role required: admin, security, user, backup-operator, none.

`ddboost fc show stats [endpoint` *`endpoint-spec`*`] [initiator` *`initiator-spec`*`] [interval` *`interval`*`] [count` *`count`*`]`
Show DD Boost Fibre Channel detailed statistics periodically based on filter. The interval is an optional number of seconds with a minimum of 1 and a maximum of 4294967295. The count is an optional ordinal value with a minimum of 1 and a maximum of 4294967295.

Role required: admin, security, user, backup-operator, none.

`ddboost fc status`
Show DD Boost Fibre Channel status. Output includes information on admin state and process state.

Role required: admin, security, user, backup-operator, none.

`ddboost fc trace disable [component {all |` *`component-list`*`}]`
Disable DD Boost Fibre Channel tracing.

Role required: admin.

`ddboost fc trace enable [component {all |` *`component-list`*`}] [level {all | high | medium | low}]`
Enable DD Boost Fibre Channel tracing.

Role required: admin.

`ddboost fc trace show [component {all |` *`component-list`*`}]`
Show DD Boost Fibre Channel trace status.

Role required: admin, security, user, backup-operator, none.

ddboost file-replication

`ddboost file-replication option reset {low-bw-optim | encryption | ipversion }`

Reset to default file-replication options. Reset low-bandwidth optimization or encryption to the default value (disabled). Reset IP version to the default value (ipv4).

Note

Low-bandwidth optimization is not supported on DD Extended Retention systems.

Role required: admin.

`ddboost file-replication option set encryption {enabled | disabled}`
Enable or disable encrypted data transfer for DD Boost file-replication. This command must be entered on both systems—the source system and the destination (target) system.

Role required: admin.

`ddboost file-replication option set ipversion {ipv4 | ipv6}`
Set the preferred IP version for DD Boost file-replication. If the ipversion option is ipv6, IPv6 is the preferred IP address type for managed file-replication. If the ipversion option is ipv4, then IPv4 is the preferred IP address type for managed file-replication. If a preferred IP address is not specified, the default is IPv4. This command must be entered on both systems—the source system and the destination (target) system.

Role required: admin.

`ddboost file-replication option set low-bw-optim {enabled | disabled}`
Enable or disable low bandwidth optimization for DD Boost. This command must be entered on both systems—the source system and the destination (target) system. Default setting is disabled.

Note

Low-bandwidth optimization is not supported on DD Extended Retention systems.

Role required: admin.

`ddboost file-replication option show [encryption]`
Show state of encryption: enabled or disabled.

Role required: admin, security, user, backup-operator, none.

`ddboost file-replication option show [ipversion]`
Show IP version options: IPv4 or IPv6.

Role required: admin, security, user, backup-operator, none.

`ddboost file-replication option show [low-bw-optim]`
Show state of low bandwidth optimization: enabled or disabled.

Role required: admin, security, user, backup-operator, none.

`ddboost file-replication reset stats`
Clear file-replication statistics when DD Boost is enabled.

Role required: admin.

`ddboost file-replication show active [all | storage-unit` *`storage-unit`* `| tenant-unit` *`tenant-unit`*`]`
Show the status of a DD Boost file-replication to destination Data Domain systems. Output for low-bandwidth optimization shows the function as enabled and running, or as enabled/off which means a configuration mismatch with the other side.

Role required: admin, security, user, backup-operator, none, tenant-admin, tenant-user.

`ddboost file-replication show detailed-file-history [all | storage-unit` *`storage-unit`* `| tenant-unit` *`tenant-unit`*`] [duration` *`duration`*`{day | hr}]`
Show a detailed, file-based replication history. Data for each file name is organized by date, time, and direction (outbound or inbound). The remote hostname is included in the output. The duration of the day and hour must be entered without a space, for example, `10day` or `5hr`. In DD OS Release 5.4.1.0, a new column —`Post-synthetic-optim`— is added to the command outputs to provide statistics for synthetic replication.

Role required: admin, security, user, backup-operator, none, tenant-admin, tenant-user.

`ddboost file-replication show detailed-history [duration` *`duration`*`{day | hr}] [interval` *`interval`* `{hr}]`
Show a detailed, cumulative view of file-replication history. Data is organized by date, time, and direction (outbound or inbound). The duration of the day and hour must be entered without a space, for example, `10day` or `5hr`. In DD OS Release 5.4.1.0, a new column —`Post-synthetic-optim`— is added to the command outputs to provide statistics for synthetic replication.

Role required: admin, security, user, backup-operator, none, tenant-admin, tenant-user.

`ddboost file-replication show file-history [all | storage-unit` *`storage-unit`* `| tenant-unit` *`tenant-unit`*`] [duration` *`duration`*`{day | hr}]`
Show the data-transfer history of inbound and outbound traffic for files in the Data Domain system `/backup` directory. The remote hostname is included in the output. The duration of the day and hour must be entered without a space, for example, `10day` or `5hr`.

Role required: admin, security, user, backup-operator, none, tenant-admin, tenant-user.

Note

There is a discrepancy between the network bytes output of the CLI and the network bytes output of the GUI. This is because the CLI reports only one direction of network bytes for `Network (KB)`, and the SMS report used by the GUI reports the sum of `network_bytes_in + network_bytes_out` for `Network Bytes (MiB)`.

`ddboost file-replication show history [duration` *`duration`*`{day | hr}] [interval` *`interval`*`{hr}]`
Show the data transfer history between the source and destination Data Domain systems. The duration of the day and hour must be entered without a space, for example, `10day` or `5hr`.

Role required: admin, security, user, backup-operator, none.

`ddboost file-replication show performance [interval` *`sec`*`] [count` *`count`*`]`
Show in real time the amount of pre-compressed outbound and inbound data compared to network throughput or post-compressed data. The count displays the number of lines equal to the count value. Output is shown for the specified interval.

Role required: admin, security, user, backup-operator, none.

Example 29

The following example displays the output of a Data Domain system which is the source and is replicating to another Data Domain system. Therefore, the source is set only for outgoing replication. For some of the time periods shown, no data was actually sent. If inbound replication traffic was set, then the columns under inbound would be filled in

Example 29 (continued)

similarly. The `ddboost file-replication show performance` command is used without any options:

```
# ddboost file-replication show performance
01/14 08:48:05
       Outbound                Inbound
 Pre-comp    Network     Pre-comp    Network
  (KB/s)     (KB/s)       (KB/s)     (KB/s)
 ---------  ---------    ---------  ---------
    165521        442            -          -
   2245638       6701            -          -
         -          -            -          -
    906275       2677            -          -
   1280554       3801            -          -
         -          -            -          -
   2386719       7046            -          -
    294790        899            -          -
         -          -            -          -
   2491855       7383            -          -
         -          -            -          -
         -          -            -          -
   1459252       4323            -          -
         -          -            -          -
         -          -            -          -
   2556742       7575            -          -
```

Note

Managed file replication statistics are populated under the `ddboost file-replication show performance` command and kept separate from the backup and restore stream stats.

Note

Managed file replication statistics are populated under the `ddboost file-replication show stats` command and kept separate from the backup and restore stream stats.

`ddboost file-replication show stats`
Monitor outbound and inbound traffic on a Data Domain system during replication. Compression ratio increases when low-bandwidth optimization is enabled.

In DD OS Release 5.4.1.0, a new row —`Bytes after synthetic optimization`— is added to the command outputs to provide statistics for synthetic replication.

Role required: admin, security, user, backup-operator, none.

Example 30

The following example displays the output of a Data Domain system which is logging the inbound replication traffic:

```
# ddboost file-replication show stats
Direction:                              Outbound
```

Example 30 (continued)

```
Network bytes sent:                         0
Pre-compressed bytes sent:                  0
Bytes after synthetic optimization:         0
Bytes after filtering:                      0
Bytes after low bandwidth optimization:     0
Bytes after local compression:              0
Compression ratio:                          0

Direction:                                  Inbound
Network bytes received:                     292,132,082,144
Pre-compressed bytes received:              36,147,804,001,570
Bytes after synthetic optimization:         36,147,804,001,570
Bytes after filtering:                      1,664,434,329,750
Bytes after low bandwidth optimization:     1,664,434,329,750
Bytes after local compression:              179,887,419,678
Compression ratio:                          123.7
```

ddboost ifgroup

`ddboost ifgroup add` *`group_name`* `{interface {`*`ipaddr`* | *`ipv6addr`*`} | client` *`host`*`}`

Add an interface, client, or both to *group-name* or to the default group. Prior to adding an interface you must create the *group_name* unless the group name is the default group. Role required: admin.

This command provides full ifgroup support for static IPv6 addresses, providing the same capabilities for IPv6 as for IPv4. Concurrent IPv4 and IPv6 client connections are allowed. A client connected with IPv6 sees IPv6 ifgroup interfaces only. A client connected with IPv4 sees IPv4 ifgroup interfaces only. Individual ifgroups include all IPv4 addresses or all IPv6 addresses. The default group behaves in the same manner as any other group.

Note

- The group-name “default” is created during an upgrade of a fresh install and is always used if *group_name* is not specified.
- You can enforce private network connectivity, ensuring that a failed job does not reconnect on the public network after network errors. When interface enforcement is enabled, a failed job can only retry on an alternative private network IP address. Interface enforcement is only available for clients that use ifgroup interfaces.

  Interface enforcement is off (FALSE) by default. To enable interface enforcement, you must add the following setting to the system registry:

  `system.ENFORCE_IFGROUP_RW=TRUE`

  After you've made this entry in the registry, you must do a `filesys restart` for the setting to take effect. For more information, see the *EMC Data Domain Boost Administration Guide*.
- An ifgroup client is a member of a single ifgroup *group-name* and may consist of a fully qualified domain name (FQDN) such as `ddboost.datadomain.com`, wild cards such as `*.datadomain.com` or “`*`”, a short name such as ddboost, or IP range of the client (`xx.xx.xx.0/24` for IPv4 or `xxxx::0/112` for IPv6). When a client's source IP address is evaluated for access to the ifgroup, the order of precedence is:

  1. Client Name: `abc-11.d1.com`
  2. Client Domain Name: `*.d1.com`
  3. All Clients: `*`
  4. IP address of the connected Data Domain system
  5. Connected client IP range. This host-range check is useful for separate VLANs with many clients where there isn't a unique partial hostname (domain).

  If none of these checks find a match, ifgroup interfaces are not used for this client.

  For detailed information about this order of precedence, see the *EMC Data Domain Boost Administration Guide*.
- By default, the maximum number of groups is eight. It is possible to increase this number by editing the system registry and rebooting.

Additionally, the IP address must be configured on the Data Domain system and its interface must be enabled. You can add public or private IP addresses for data transfer connections. After adding an IP address as an interface, you can enable advanced load balancing and link failover.

See the *EMC Data Domain Boost Administration Guide* and the *EMC Data Domain Operating System Administration Guide* for more information on interface groups.

`ddboost ifgroup create` *`group-name`*

Create a group with the name *group-name* for the interface. Group names may contain alphanumeric characters, hyphens, and underscores. System hostnames, fully qualified hostnames, and wildcard hostnames indicated by an asterisk may also be used. Reserved group names that cannot be used are **`default`**, **`all`**, or **`none`**. Role required: admin.

`ddboost ifgroup del` *`group_name`* `{interface {`*`ipaddr`* `|` *`ipv6addr`*`} | client` *`host`*`}`

Remove an interface, client, or both from *group_name* or default group. Deleting the last IP address interface disables the ifgroup. If this is the case, you have the option of terminating this command option. Role required: admin.

`ddboost ifgroup destroy` *`group-name`*

Destroy the group name. Only empty groups can be destroyed. Interfaces or clients cannot be destroyed but may be removed sequentially or by running the command option ddboost ifgroup reset *group-name*. Role required: admin.

Note

The group-name “default” cannot be destroyed.

`ddboost ifgroup disable` *`group-name`*

Disable a specific group by entering the *group-name*. If *group-name* is not specified, the command applies to the default group. Role required: admin.

`ddboost ifgroup enable` *`group-name`*

Enable a specific group by entering the *group-name*. If *group-name* is not specified, the command applies to the default group. Role required: admin.

`ddboost ifgroup rename` *`source-group-name destination-group-name`*

Rename the ifgroup *source-group-name* to *destination-group-name*. This command option does not require disabling the group. The default group cannot be renamed. Role required: admin.

`ddboost ifgroup reset` *`group-name`*

Reset a specific group by entering the *group-name*. If *group-name* is not specified, the command applies to the default group. Role required: admin.

`ddboost ifgroup show config {interfaces | clients | groups | all} [`*`group-name`*`]`

Display selected configuration options. If no selection is made, all information about the specified *group-name* is shown. Role required: admin, security, user, backup-operator, none.

If *group-name* is not specified, information for all the groups is shown. Select the all argument to view configuration options of all groups. All users may run this command option.

`ddboost ifgroup status` *`group-name`*

Show status of the specified *group-name*: enabled or disabled. Role required: admin, security, user, backup-operator, none.

If *group-name* is not specified, status for the default group is shown. All users may run this command option.

ddboost option

`ddboost option reset {distributed-segment-processing | virtual-synthetics | fc}`

Reset distributed segment processing, virtual synthetics to the default option of enabled. Reset Fibre Channel to the default option of disabled. Virtual synthetics and Fibre Channel features are supported on single-node configurations and systems with Extended Retention only.

Role required: admin.

`ddboost option set distributed-segment-processing {enabled | disabled}`

Enable or disable the distributed segment processing feature on DD Boost. Distributed-segment-processing feature is supported on single-node configurations and systems with Extended Retention only.

Role required: admin.

`ddboost option set fc {enabled | disabled}`
Enable or disable Fibre Channel for DD Boost. Fiber Channel features are supported on single-node configurations and systems with Extended Retention.

Role required: admin.

`ddboost option set virtual-synthetics {enabled | disabled}`
Enable or disable the virtual synthetics feature on the DD Boost. Virtual synthetics features are supported on single-node configurations and systems with Extended Retention.

Role required: admin.

`ddboost option show [distributed-segment-processing | virtual-synthetics | fc]`
Show status of distributed segment processing, virtual synthetics, or Fibre Channel. If no argument is specified, status for all arguments are shown. Status is enabled or disabled. Default is enabled for distributed segment processing and virtual synthetics. Default is disabled for Fibre Channel. All users may run this command.

Role required: admin, security, user, backup-operator, none.

ddboost reset

`ddboost reset stats`
Reset statistics when DD Boost is enabled, or as a network recovery procedure to clear job connections after the network connection is lost.

Role required: admin.

`ddboost reset user-name` *`user-name`*
This command is deprecated. Use `ddboost user unassign` command instead.

Role required: admin.

ddboost set

`ddboost set user-name` *`user-name`*
This command is deprecated. Use `ddboost user assign` command instead.

Note

The `ddboost user assign` command will be the default command to create users for DD Boost storage units.

Role required: admin.

ddboost show

`ddboost show connections [detailed]`
Show DD Boost active clients and client connections. Client information includes name, idle status, plug-in version, OS version, application version, encryption, DSP, and transport. Using the `detailed` option provides CPU and memory data.

Role required: admin, security, user, backup-operator, none.

Note

- When DD Boost Fibre Channel is enabled, connections are listed in the category Interfaces and are named DDBOOST_FC. The ifgroup Group Name category does not apply to DD Boost Fibre Channel; therefore, the group name is listed as n/a.
- AIR replication job count will be displayed as a `Src-repl` job in the output of a `ddboost show connections` command, the same as other NetBackup and Backup Exec optimized duplication jobs.
- Only IPv4 addresses can be configured for `ifgroup`; IPv6 cannot be configured.
- Both the control connection for file replication and the actual replication interfaces are displayed.

Example 31

The following example displays the output of a `ddboost show connections` command.

```
Active Clients: 1

Clients:
Client                        Idle   Plugin Version                      OS Version   Application Version   Encrypted   DSP   Transport
---------------------------   ----   --------------   --------------------------------   ------------------   ---------   ---   ---------
rtp-ost-ms02.datadomain.com   NO           3.0.1.0-   Linux 2.6.32-71.el6.x86_64 x86_64     ddpconnchk client          NO   YES         IPv4
---------------------------   ----   --------------   --------------------------------   ------------------   ---------   ---   ---------

Client Connections:
Max Client Connections: 180
-------------- ifgroup ---------------------------------   ---------------- Client Connections -----------   - DD Connections -   -----
                                                           ----- Control -----                ------ Data ------
Group-name   Status                          Interface   Write   Read   Src-repl   Dst-repl   Synthetic   Repl-out   Repl-in   Total
----------   -------   ---------------------------------   -----   ----   --------   --------   ---------   --------   -------   -----
none                                        10.6.109.41       0      0          0          0           0          0         0       0
none                  2620:0:170:1604:215:17ff:fea0:eaf4      0      0          0          0           0          0         0       0
none                  2620:0:170:1604:215:17ff:fea0:eaf5      0      0          0          0           0          0         0       0
none                                         3000::230      0      0          0          0           0          0         0       0
none                                         3000::231      0      0          0          0           0          0         0       0
none                  2620:0:170:1604:21b:21ff:fe5f:e628      0      0          0          0           0          0         0       0
none                  2620:0:170:1604:21b:21ff:fe5f:e629      0      0          0          0           0          0         0       0
none                  2620:0:170:1604:21b:21ff:fe5f:e62c      0      0          0          0           0          0         0       0
none                  2620:0:170:1604:21b:21ff:fe5f:e62d      0      0          0          0           0          0         0       0
default      enabled                        10.6.109.40      0      0          0         15           0          0        15      30
10GLab       disable                     192.168.1.230       0      0          0          0           0          0         0       0
10GLab       disable                     192.168.1.231       0      0          0          0           0          0         0       0
only1G       enabled                      10.6.109.244       0      0          0          0           0          0         0       0
only1G       enabled                      10.6.109.144       0      0          0          0           0          0         0       0
only1G       enabled                      10.6.109.145       0      0          0          0           0          0         0       0
only1G       enabled                      10.6.109.146       0      0          0          0           0          0         0       0
----------   -------   ---------------------------------   -----   ----   --------   --------   ---------   --------   -------   -----
                                    Total Connections:       0      0          0         15           0          0        15      30
----------   -------   ---------------------------------   -----   ----   --------   --------   ---------   --------   -------   -----
```

`ddboost show histogram`

Display a DD Boost histogram for the Data Domain system.

Role required: admin, security, user, backup-operator, none.

Output Definitions

mean
The mathematical mean time for completion of the operations, in milliseconds.

std-dev
The standard deviation for time to complete operations, derived from the mean time, in milliseconds.

‹1ms
The number of operations that took less than 1 millisecond.

‹5ms
The number of operations that took between 1 milliseconds and 5 milliseconds.

‹10ms
The number of operations that took between 5 milliseconds and 10 milliseconds

‹100ms
The number of operations that took between 10 milliseconds and 100 milliseconds.

‹1s
The number of operations that took between 100 milliseconds and 1 second.

‹10s
The number of operations that took between 1 second and 10 seconds.

‹10s
The number of operations that took less than 10 seconds.

›10s
The number of operations that took more than 10 seconds.

total
The total time taken for a single operation, in milliseconds.

max
The maximum time taken for a single operation, in milliseconds.

min
The minimum time taken for a single operation, in milliseconds.

Example 32

```
# ddboost show histogram
07/23 09:43:16

-----------------------------------------------------------------
OPER         mean    std-dev   <1ms    <5ms   <10ms  <100ms ...
-----------------------------------------------------------------
...
DDP_GETATTR 0.00ms   0.00ms      0       0       0       0 ...
DDP_LOOKUP  3.34ms  29.17ms  13389     126     137     617 ...
DDP_WRITE   0.30ms   4.98ms  125...   5048    1776    1502 ...
...
```

`ddboost show stats [ interval` *seconds* `] [count` *count*`]`
Show DD Boost statistics. The interval is an optional number of seconds with a minimum of 1 and a maximum of 4294967295. The count is an optional ordinal value with a minimum of 1 and a maximum of 4294967295.

Role required: admin, security, user, backup-operator, none.

Example 33

```
# ddboost show stats
07/08 14:54:09

DD Boost statistics:
OPER                                          Total    Failed
DDP_GETATTR                             :        91       [0]
....
```

Example 33 (continued)

```
DDP_PATHCONF                          :              0         [0]
DDP_SYNC                              :              0         [0]
DDP_COMPSTATS                         :              0         [0]
DDP_GET_DFC_ATTR                      :              0         [0]

DDP_SSL_QUERY                         :            117         [0]

DDP_REMFILECREATE                     :              0         [0]
...
```

`ddboost show user-name`
This command is deprecated. Use `ddboost user show` command instead.

The output will display the default DD Boost user if one is configured, otherwise, the output will display that there is no default user.

Role required: admin, security, user, backup-operator, none.

ddboost status

`ddboost status`
Display status of DD Boost: enabled or disabled.

Role required: admin, security, user, backup-operator, none.

ddboost storage-unit

`ddboost storage-unit create` *`storage-unit`* `user` *`user-name`* `[tenant-unit` *`tenant-unit`*`] [quota-soft-limit` *`n`* `{MiB|GiB|TiB|PiB}] [quota-hard-limit` *`n`* `{MiB|GiB|TiB|PiB}] [report-physical-size` *`n`* `{MiB|GiB|TiB|PiB}] [write-stream-soft-limit` *`n`*`] [read-stream-soft-limit` *`n`*`] [repl-stream-soft-limit` *`n`*`] [combined-stream-soft-limit` *`n`*`]`
Create a storage unit, assign tenant, and set quota limits.

Note

If the quota feature is not enabled, the quota is created but a message appears stating the feature is disabled and quota limits are not enforced.

Note

The `tenant-unit` option is introduced for integration with the Secure Multi-Tenancy feature. For more information about this feature, refer to the EMC Data Domain Secure Multi-Tenancy User's Guide.

Role required: admin.

Storage unit names can be up to 50 characters. Naming conventions for creating storage units include upper case and lower case letters—A-Z and a-z, numbers 0-9, embedded space, comma, period, exclamation mark, hash mark, dollar sign, percent sign, plus sign, at sign, equal sign, ampersand, semi colon, caret, tilde, left and right parentheses, left and right brackets, left and right braces.

Quotas may cause OpenStorage backup applications to report unexpected sizes and capacities. See Knowledge Base article 85210, available on the EMC Online Support.

`ddboost storage-unit delete` *`storage-unit`*
Delete a specified storage unit, its contents, and any DD Boost associations. The deleted storage-unit retains its old name and is shown as deleted in the mtree list.

Note

You must also manually remove (expire) corresponding catalog entries from the backup application.

Role required: admin.

`ddboost storage-unit modify` *`storage-unit`* `[user` *`user-name`*`] [tenant-unit {`*`tenant-unit`* `| none}] [quota-soft-limit {`*`n`* `{MiB|GiB|TiB|PiB} | none}] [quota-hard-limit {`*`n`* `{MiB|GiB|TiB|PiB} | none}] [report-physical-size {`*`n`* `{MiB|GiB|TiB|PiB} | none}] [write-stream-soft-limit {`*`n`* `| none}] [read-stream-soft-limit {`*`n`* `| none}] [repl-stream-soft-limit {`*`n`* `| none}] [combined-stream-soft-limit {`*`n`* `| none}]`
Modify storage-unit user, tenant, and quota limits.

Role required: admin.

If DD Boost storage units are replicated with MTree or collection replication, each storage unit on the target must have the DD Boost user added with the command `ddboost storage-unit modify` before being accessed by the Boost backup software. The following example sets the user of the storage unit **`STU1`** to **`ostuser`**.

```
# ddboost user show
ostuser
Assuming storage-unit STU1
# ddboost storage-unit modify STU1 user ostuser
```

The example below shows that a nonexistent storage-unit cannot be modified:

```
# ddboost storage-unit modify hello user user5

**** Failed to find storage-unit
```

`ddboost storage-unit rename` *`storage-unit new-storage-unit`*
Rename a storage-unit while maintaining its:

- Username ownership
- Stream limit configuration
- Capacity quota configuration and physical reported size
- AIR association on the local Data Domain system

Note

- A ddboost association on a remote host must be corrected manually.
- You cannot use this command to rename an Mtree.

Role required: admin.

The example below shows the renaming of a storage-unit:

```
# ddboost storage-unit rename task1 tasking1
storage-unit "task1" renamed to "tasking1".
```

`ddboost storage-unit show [compression] [`*`storage-unit`*`] [tenant-unit `*`tenant-unit`*`]`

Lists storage-units assigned to tenant-unit and images in a storage-unit. Displays the compression for all storage units (the original byte size, global and local compression) or the filenames in a specified storage unit. The list of files in a storage unit is shown in the output only if a storage unit name is specified. This command can filter on a specific storage-unit or tenant-unit.

Role required: admin, security, user, backup-operator, none, tenant-admin, tenant-user.

The example below displays the list of storage-units:

```
# ddboost storage-unit show
Name                 Pre-Comp (GiB)   Status   User       Report Physical   Tenant-Unit
                                                             Size (MiB)
-----------------   --------------   ------   --------   ---------------   -----------
backup                          3.0   RW       sysadmin                -   -
DDBOOST_STRESS_SU              60.0   RW       sysadmin                -   -
task2                           0.0   RW       sysadmin                -   -
tasking1                        0.0   RW       sysadmin                -   -
DD1                             0.0   RW       sysadmin                -   -
D6                              5.0   RW       sysadmin                -   -
TEST_DEST                       0.0   RW       sysadmin                -   -
STU-NEW                         0.0   RW       ddu1                    -   -
getevent                        0.0   RW       ddu1                    -   -
DDP-5-7                       120.0   RW       sysadmin                -   -
TESTME                        150.0   RW       sysadmin                -   -
DDP-5-7-F                     100.0   RW       sysadmin                -   -
testSU                          0.0   RW       sysadmin              200   -
-----------------   --------------   ------   --------   ---------------   -----------
Q    : Quota Defined
RO   : Read Only
RW   : Read Write
RD   : Replication Destination
```

`ddboost storage-unit undelete` *storage-unit*

Recover a deleted storage-unit including its:

- Username ownership
- Stream limit configuration
- Capacity quota configuration and physical reported size
- AIR association on the local Data Domain system

Note

- Deleted storage units are available until the next `filesys clean` command is run.
- You cannot use this command to undelete an Mtree.
- You cannot use this command to undelete a storage unit deleted using the DD Boost SDK. To recover a storage unit deleted using the DD Boost SDK:
  1. Enter `mtree show` to determine which deleted mtree is the storage unit to be undeleted. Look in `messages.engineering` to find the renamed value.
  2. Enter `ddboost storage-unit undelete` deleted-*xxxxxxxx*, where deleted-*xxxxxxxx* is the name of the deleted storage unit identified in the first step.
  3. Enter `ddboost rename` deleted-*xxxxxxxx SU_NAME*, where *SU_NAME* is the storage unit being recovered.

Role required: admin.

The example below shows the recovery of a deleted storage-unit:

```
# ddboost storage-unit undelete task1
Storage-unit "task1" undeleted successfully.
```

ddboost streams

`ddboost streams show active [all | storage-unit` *`storage-unit`* `| tenant-unit` *`tenant-unit`*`]`

Displays active streams per storage-unit.

Role required: admin, security, user, backup-operator, none, tenant-admin, tenant-user.

Example 34

```
# ddboost streams show active

Name  Read     Write   Repl-out  Repl-in  Read   Write   Repl
Combined
      Streams  Streams Streams   Streams  Limit  Limit   Limit  Limit
----  -------  ------- --------  -------  -----  -----  -----
--------
stu1    0         0       0          0      2      3       -
-
stu2    0         0       0          0      -      -       -
-
----  -------  ------- --------   ------- -----  -----   -----
--------
DD System Stream Limits: read=4 write=16 repl-in=20 repl-out=15
combined=16
```

Note

The DD system stream limits above are based on the type of the DD system.

The system administrator configures stream warning limits against each storage-unit for each of the four limits: backup, restore, replication and combined streams. When any stream count exceeds the warning limit quota, an alert is generated. The alert automatically clears once the stream limit returns below the quota for over 10 minutes.

Note

DD Boost users are expected to reduce the workload to remain below the stream warning quotas or the system administrator can change the warning limit configured to avoid exceeding the limit.

To create a storage unit with stream limits, enter:

```
# ddboost storage-unit create NEW_STU0 user user2 write-stream-soft-
limit 5
read-stream-soft-limit 1 repl-stream-soft-limit 2
Created storage-unit "NEW_STU0" for "user2".
Set stream warning limits for storage-unit "NEW_STU0".
```

To modify the stream limits for storage units, enter:

```
# ddboost storage-unit modify NEW_STU1 write-stream-soft-limit 3
read-stream-soft-limit 2 repl-stream-soft-limit 1
NEW_STU1: Stream soft limits: write=3, read=2, repl=1, combined=none
```

`ddboost streams show history {storage-unit` *`storage-unit`* `| tenant-unit` *`tenant-unit`*`} [interval` *`mins`*`] [last`*`n`* `{hours | days | weeks | months} | start` *`MMDDhhmm[[CC]YY]`* `[end` *`MMDDhhmm[[CC]YY]`*`]]`

Displays streams history per storage-unit or a list of storage-units associated with a tenant-unit.

Role required: admin, security, user, backup-operator, none, tenant-admin, tenant-user.

Example 35

```
# ddboost streams show history storage-unit stu1 last 1hours
INTERVAL: 10 mins
"-" indicates that the data is not available for the intervals

Storage-Unit: "stu1"
Date        Time    read      write     repl-out    repl-in
YYYY/MM/DD  HH:MM   streams   streams   streams     streams
---------- -------  -------  -------  ---------  --------
2013/08/29  12:00     0         0         0           0
2013/08/29  12:10     0         0         0           0
2013/08/29  12:20     0         1         0           0
2013/08/29  12:30     0         2         0           0
2013/08/29  12:40     0         2         0           0
2013/08/29  12:50     0         1         0           0
2013/08/29  13:00     0         0         0           0
---------- ------   -------   -------   ---------   --------

# ddboost streams show history storage-unit stu12
Storage-unit /data/col1/stu12 not configured
```

ddboost user

`ddboost user assign` *`user-name-list`*

Assign Data Domain system users to the list of recognized DD Boost users. Role required: admin, security, user, backup-operator, none, tenant-admin, tenant-user.

This command is typically used for applications that create storage-units through the DD Boost SDK APIs.

Note

When a storage-unit is created with a valid Data Domain system local user that is not assigned to DD Boost, the user is automatically added to the DD Boost user list.

Example 36

```
# ddboost user assign user1 user2
User "user1" assigned to DD Boost.
User "user2" assigned to DD Boost.

# ddboost user show
DD Boost user
-------------
user1
user2
-------------

# ddboost user unassign user1
User "user1" unassigned from DD Boost.
```

`ddboost user option reset` *user-name* `[default-tenant-unit]`
Unassign DD Boost user *user-name* from `default tenant-unit`. This command removes DD Boost user *user-name* from the list of valid users for DD Boost. However, this command does not unassign a user if the user is still the owner of a storage-unit. Role required: admin.

Example 37

The following output displays how to set the tenant-units when working with Secure Multi-Tenancy. (The default tenant-unit is displayed only when Secure Multi-Tenancy is enabled.)

```
# smt tenant-unit create tu2
Tenant-unit "tu2" created.
# ddboost user option set user2 default-tenant-unit tu2
Default-tenant-unit is set to "tu2" for user "user2".

# ddboost user show
DD Boost user   Default tenant-unit
-------------   -------------------
user2           tu2
-------------   -------------------

# ddboost user option reset user2
Default-tenant-unit is reset for user "user2".
```

`ddboost user option set` *user* `default-tenant-unit` *tenant-unit*
Set the default tenant-unit for the specified DD Boost user. When a storage-unit is created with a user, the tenant-unit is automatically associated with that user. Role required: admin, security, user, backup-operator, none, tenant-admin, tenant-user.

`ddboost user show` *user* `[default-tenant-unit` *tenant-unit*`]`
List DD Boost users and their default tenant-units. You can use the `ddboost user assign` command or the `ddboost storage-unit create user` command to assign users. Role required: admin, security, user, backup-operator, none, tenant-admin, tenant-user.

Example 38

```
# ddboost user show

DD Boost user   Default tenant-unit
-------------   -------------------
ddbu1           -
ddbu2           -
ddu1            -
sysadmin        -
tu1             -
-------------   -------------------
```

`ddboost user unassign` *user-name*
Unassign a user from the DD Boost user list. This command deletes the user from the DD Boost users list. A user can only be deleted when it does not own any storage-units. Role required: admin, security, user, backup-operator, none, tenant-admin, tenant-user.

Note

The `ddboost user unassign` command does not validate the DD Boost user, it only looks to see if the user has been previously assigned to the DD Boost users list.

Example 39

If the administrator is trying to delete a specific user named `user4`, who has not been previously assigned to the users list, by either using the `ddboost user unassign` or `ddboost user option reset` command, then the following output will display that this user is not assigned to the DD Boost users list:

```
# ddboost user unassign user4
*** User "user4" is not assigned to DD Boost.

# ddboost user option reset tenant4
*** User "tenant4" is not assigned to DD Boost.
```

CHAPTER 11

disk

The `disk` command manages disks and displays disk locations, logical (RAID) layout, usage, and reliability statistics. Each Data Domain system reports on the number of disks in the system. For a Data Domain system with one or more Data Domain external disk shelves, commands also include entries for enclosures and disks.

This chapter contains the following topics:

disk Change History

This section provides a list of changes since the 5.4 release, for all 5.5.x releases, in order of most recent release to first release.

Modified Arguments in DD OS 5.5

disk beacon *enclid.diskid*

Added the option to specify the target disk with a serial number.
`disk beacon {`*`enclid.diskid`* `|` *`serialno`*`}`

Modified Output in DD OS 5.5

disk beacon *enclid.diskid*

The output now includes the slot number. For example, `Start disk LED beaconing for 1.1 at slot 1 ...`

Deleted Commands in DD OS 5.5

disk multipath failback

disk multipath option set auto-failback {enabled | disabled}

disk beacon

`disk beacon {`*`enclosure-id.disk-id`* `|` *`serialno`*`}`
Cause the LED that signals normal operation to flash on the target disk. Press Ctrl-C to stop the flash. To display disk identification information, enter `disk show hardware`. To beacon all disks in an enclosure, enter `enclosure beacon`. Role required: admin.

disk fail

`disk fail` *`enclosure-id.disk-id`*
Fail a disk and force reconstruction. Role required: admin.

disk multipath

`disk multipath option reset {monitor | auto-failback}`
Disable multipath configuration monitoring. When disabled, failures in paths to disk devices do not generate alerts. Multipath configuration monitoring is disabled by default.

To perform auto-failback, use this command to switch over to the primary path when it becomes available, even if the secondary path remains usable. The auto-failback option is enabled by default and supported on gateway systems only. Role required: admin.

`disk multipath option set monitor {enabled | disabled}`
Enable multipath configuration monitoring. When enabled, failures in paths to disk devices generate alerts and log multipath events. If monitoring is disabled, multipath event logging is not performed, meaning disk multipath show history is not updated. Multipath configuration monitoring is disabled by default. Role required: admin.

`disk multipath option show`
Show status of multipath configuration monitoring and auto-failback: disabled or enabled. Auto-failback is supported on gateway systems only. Role required: admin, security, user, backup-operator, or none.

`disk multipath reset stats`
Clear statistics of all disk paths in expansion shelves. Role required: admin.

`disk multipath resume port port`
Allow I/O on specified initiator port. Role required: admin.

`disk multipath show history`
Show history of multipath events. Role required: admin, security, user, backup-operator, or none.

`disk multipath show stats [enclosure enc-id]`
Show statistics for all disk paths by default, or for the specified enclosure only.

`disk multipath status [port-id]`
Show multipath configurations and runtime status. Role required: admin, security, user, backup-operator, or none.

`disk multipath suspend port port`
Disallow I/O on specified initiator port, and stop traffic on particular ports during scheduled maintenance of the SAN, storage array, or system. This command does not drop the Fibre Channel link. Role required: admin.

disk port

`disk port enable port-id`
Enable the specified initiator port. Role required: admin.

`disk port show {stats | summary}`
Show disk port information. Role required: admin, security, user, backup-operator, or none.

disk rescan

`disk rescan [enclosure-id.disk-id]`
Rescan all disks to look for newly removed or inserted disks or LUNs or power on a drive. Role required: admin.

disk reset

`disk reset performance`
Reset disk performance statistics to zero. Role required: admin.

disk set

`disk set dev disk-id spindle-group 1-16`
Assign a LUN group to the disk. You must restart the file system after adding the LUN. Role required: admin.

disk show

`disk show failure-history`
Display list of serial numbers of failed disks in the Data Domain system. Role required: admin, security, user, backup-operator, or none.

`disk show hardware`

Display disk hardware information. The output includes a column for slot numbering. The number displayed in the Slot column is based on the type of system on which the command is run:

- Slot numbering begins at 0 on DD2500 systems.
- Slot numbering begins at 0 on systems DD4200, DD4500, and DD7200, however slot 0 is unused and does not appear in output.
- Slot numbering begins at 1 on systems DD990 and earlier.

Role required: admin, security, user, backup-operator, or none.

Output Definitions (Disk Information)

Disk (enc/disk)
The enclosure and disk numbers.

Slot
The slot number for the disk.

Manufacturer/Model
The manufacturer model designation.

Firmware
The firmware revision on each disk.

Serial No.
The manufacturer serial number for the disk.

Capacity
The data storage capacity of the disk when used in a Data Domain system. The Data Domain convention for computing disk space defines one gigabyte as 230 bytes, giving a different disk capacity than the manufacturer's rating.

Type
The type of disk drive.

Output Definitions (System Information)

Disk
Each LUN accessed by the Data Domain system as a disk.

LUN
The LUN number given to a LUN on the third-party physical disk storage system.

Port WWN
The world-wide number of the port on the storage array through which data is sent to the Data Domain system.

Manufacturer/Model
A label that identifies the manufacturer. The display may include a model ID, RAID type, or other information depending on the vendor string sent by the storage array.

Firmware
The firmware level used by the third-party physical disk storage controller.

Serial No.
The serial number from the third-party physical disk storage system for a volume that is sent to the Data Domain system.

Capacity
The amount of data in a volume sent to the Data Domain system. GiB = Gibibytes, the base-2 equivalent of Gigabytes. MiB = Mebibytes, the base-2 equivalent of Megabytes. TiB = Tebibytes, the base-2 equivalent of Terabytes.

Spindle-Group
The spindle-group for this LUN. (Available on gateway systems only.)

`disk show performance`

Display disk performance statistics for each disk. Each column displays statistics averaged since the last `disk reset performance` command or the last system power cycle.

Command output from a gateway Data Domain system lists each LUN accessed by the Data Domain system as a disk. Role required: admin, security, user, backup-operator, or none.

Output Definitions

Disk (enc/disk)
The enclosure and disk numbers.

Read sects/s
The average number of sectors per second written to each disk.

Write sect/s
The average number of sectors per second written to each disk.

Cumul. MiBytes/s
The average number of megabytes per second written to each disk. MiBytes = MiB = Mebibytes, the base-2 equivalent of Megabytes.

Busy
The average percent of time that each disk has at least one command queued.

`disk show reliability-data`

View details of the hardware state of each disk. Output also includes the operational state of drives and if the drive is present or absent. Output is typically used by Data Domain Support for troubleshooting assistance. Role required: admin, security, user, backup-operator, or none.

Output Definitions

Disk
The enclosure.disk-id disk identifier.

Slot
The disk slot number.

ATA Bus CRC Err
The uncorrected raw UDMA CRC errors.

Reallocated Sectors
The number of mapped-out defective sectors.

Temperature
The current temperature of each disk in Celsius and Fahrenheit. The allowable case temperature range for disks is from 5 degrees centigrade to 55 degrees centigrade.

`disk show state`

Display state information for all disks in an enclosure (a Data Domain system or an attached expansion shelf) or LUNs in a Data Domain gateway system using storage area network (SAN) storage.

If a RAID disk group reconstruction is underway, columns for the disk identifier, progress, and time remaining are included in command output. Role required: admin, security, user, backup-operator, or none.

Disk State Definitions

The following describes the symbols that define the state of each disk:

.
(Period) In Use

A
Absent

C
Copy Recovery Disks

D
Disabled

E
Error Disks

K
Known

O
Foreign

P
Powered Off

R
Reconstruction

s
Spare

U
Unknown

v
Available

Y
System

disk status

`disk status`
View details on the Data Domain system disk status. Output includes the number of disks in use and failed, the number of spare disks available, and if a RAID disk group reconstruction is underway.

Note

The RAID portion of the display could show one or more disks as Failed while the Operational portion of the display could show all drives operating nominally. A disk can be physically functional and available, but not in use by RAID, possibly because of user intervention.

On a gateway Data Domain system, the display shows only the number and state of the LUNs accessed by the Data Domain system. The remainder of the display is invalid for a gateway system.

Reconstruction is done per disk. If more than one disk is to be reconstructed, the disks queued for reconstruction show as spare or hot spare until reconstruction begins.

In the first line of output, disk status is indicated by one of the following, high-level states.

Normal
System is operational and all disks are available and ready for use.

Error
A new head unit is in this state when Foreign storage is present. For a system configured with some storage, Error indicates that some or all of its own storage is missing.

Warning
A special case of a system that would have been Normal if the system had none of the following conditions that require user action:

- RAID system degraded
- Foreign storage
- Failed or Absent disks

Role required: admin, security, user, backup-operator, or none.

disk unfail

`disk unfail` *`enclosure-id.disk-id`*

This command option makes a disk previously marked Failed or Foreign usable to the system. Role required: admin.

CHAPTER 12

enclosure

The `enclosure` command identifies and displays information about Data Domain system enclosures and attached expansion shelves. Beginning with 5.4, output from the `enclosure show` command option includes device VPD information for enclosures on newer Data Domain appliances (DD4500 and DD7200). VPD information enables users to monitor systems more efficiently.

This chapter contains the following topics:

enclosure Change History

This section provides a list of changes since the 5.4 release, for all 5.5.x releases, in order of most recent release to first release.

Modified Output in DD OS 5.5

`enclosure show all [`*`enclosure`*`]`

For DD2500, DD4200, DD4500, and DD7200 systems, this command now displays SLIC FRU information.

`enclosure show chassis [`*`enclosure`*`]`

For DD2500, DD4200, DD4500, and DD7200 systems, this command now displays SLIC FRU information.

enclosure Guidelines and Restrictions

- Enclosure numbers are not static and may change when the system is rebooted. (Numbers are generated according to when the shelves are detected during system startup.)
- If a Data Domain system or a previously installed shelf, or both, require spare disks and none are available, disks from a newly installed shelf are allocated to the existing RAID groups (disk groups) when the new shelf is recognized by the `disk rescan` command. The shelf allocating the disks must have at least 14 disks available for its own RAID group.

enclosure beacon

`enclosure beacon` *`enclosure`*

Confirm that the DD OS and hardware recognize an enclosure. This command option causes the LED on each disk in an enclosure to flash green, indicating activity. Press Ctrl-C to halt the command. Role required: admin.

enclosure show

`enclosure show all [`*`enclosure`*`]`

Display detailed information for all enclosures and environmentals. To view information on a specific environmental, use the `enclosure show` command and include the environmental as an argument; for example `enclosure show fans`. Environmentals included in the output of enclosure show all are:

- Fans
- Temperature
- Power-supply

(For enclosure 1 [head unit] only)

- Chassis
- IO-Cards
- Controller
- CPUs

- Memory
- NVRAM

Role required: admin, security, user, backup-operator, or none.

`enclosure show chassis [enclosure]`
Show detailed enclosure chassis inventory. To view information on a specific enclosure, include the enclosure number as the keyword. Role required: admin, security, user, backup-operator, or none.

`enclosure show controllers [enclosure]`
Display information and status for an enclosure and shelf controller systems. Role required: admin, security, user, backup-operator, or none.

Controller Definitions (Physical Enclosure Shell)

Enclosure
The number listed here is the enclosure number assigned by the Data Domain OS. (Enclosure 1 is the head unit.) This number is the argument passed to the command.

Model
The product name or appliance series of the enclosure.

Capacity
The number of usable drive slots in the enclosure.

Serial No.
The serial number of the physical enclosure. As with the WWN, this describes the enclosure and does not change if components are swapped. Depending on when the enclosure was manufactured, this may be the same value as the WWN. This value matches the serial number printed on the label on the back of the enclosure.

Number of Controllers
The number of shelf controllers currently inserted into the enclosure.

Output Definitions (Controller Modules)

Controller 1
Identifies which shelf controller module the block of information is for. If this enclosure has both shelf controllers installed, there are blocks for Controller 1 and Controller 2.

Firmware
The revision level of the firmware that resides on the shelf controller. This value can be different for each shelf controller.

Serial #
The serial number for the shelf controller. The serial number is different for each shelf controller and differs from the enclosure serial number.

Part #
The part number for the shelf controller.

Status
The current status of the shelf controller.

Type
The type of shelf controller.

`enclosure show cpus [enclosure]`
Display CPU information, such as the number of CPUs, type, and speed. Role required: admin, security, user, backup-operator, or none.

`enclosure show fans [enclosure]`

Display the current status of fans in all enclosures, or in a specific enclosure. Role required: admin, security, user, backup-operator, or none.

Output Definitions

Enclosure
The enclosure number, starting from 1, for the Data Domain system.

Description
The ID for each power or cooling unit.

Level
The fan speed. This value depends on the internal temperature and amount of cooling required.

Status
The fan status: OK or Failed.

`enclosure show io-cards [`*enclosure*`]`
Display information on device names, firmware revision, interface, slot and ports. Role required: admin, security, user, backup-operator, or none.

`enclosure show memory [`*enclosure*`]`
Show current and maximum DIMM inventory for head enclosure. Memory size is calculated in base-2 Mib. Role required: admin, security, user, backup-operator, or none.

`enclosure show nvram [`*enclosure*`]`
Displays information previously displayed by the deprecated command option `system show NVRAM`, including card number, component values (slot, memory size, errors, battery charge). If output indicates one or more component errors, an alerts notification is sent to the designated group and the Daily Alert Summary email includes an entry citing details of problem. Role required: admin, security, user, backup-operator, or none.

`enclosure show powersupply [`*enclosure*`]`
Display the status of USAF power supplies in all enclosures or in a specific enclosure. Identification corresponds to the labeled identifier on the power supply. Role required: admin, security, user, backup-operator, or none.

`enclosure show summary`
List enclosures, model and serial numbers, state, OEM names and values, and capacity (number of disks in the enclosure). The serial number for an expansion shelf is the same as the chassis serial number, which is the same as the enclosure WWN and the OPS panel WWN. Role required: admin, security, user, backup-operator, or none.

Enclosure states may be one of the following:

Offline
No connectivity to shelf. Shelf was connected previously. Also occurs if there is no power to the enclosure following startup).

Online
Operating as expected. No problems detected.

Fault
Applies to ES20 only. Indicates no communication with firmware.

Found
Transient state. Enclosure detected (though not seen by user) and will transition to other states.

Error
Hardware or software error.

Software Error
Typically means busy. Try again later.

`enclosure show temperature-sensors [`*enclosure*`]`
List the temperatures for specific system and expansion shelf components. Each Data Domain system model is configured to operate within a specific temperature range, which is defined by a temperature profile that is not configurable. If the temperature drops below or rises above the parameters defined in the profile, the system shuts down. For example, the temperature profile for some system models shuts down the system when the temperature drops below 0 degrees Celsius or rises above 80 degrees Celsius.

CPU temperatures may be shown in relative or ambient readings. Relative readings are displayed as negative numbers and indicate the difference between the current temperature and the CPU throttling point, when the CPU will reduce its power consumption. Ambient readings are displayed as positive numbers and indicate the approximate temperature of the component. A status of Critical indicates the temperature is above the shutdown threshold. Role required: admin, security, user, backup-operator, or none.

`enclosure show topology`
Show the layout of the SAS enclosures attached to a system. Role required: admin, security, user, backup-operator, or none.

enclosure test

`enclosure test topology` *port* `duration` *minutes*
Test the connections in the enclosure topology. Role required: admin.

enclosure

CHAPTER 13

filesys

The `filesys` command displays statistics, capacity, status, and use of the filesystem. Command options also clear the statistics file, and start and stop filesystem processes. The `filesys clean` command options reclaim physical storage within the filesystem. Command output for disk space or the amount of data on disks is computed using base-2 calculations. See the *EMC Data Domain Operating System Administration Guide* for details.

The `filesys archive` command option is specific to a Data Domain system with Extended Retention, and enables administrative users to provision the filesystem with tiered storage. See the *EMC Data Domain Operating System Administration Guide* for details on command usage and examples.

This chapter contains the following topics:

filesys Change History

This section provides a list of changes since the 5.4 release, for all 5.5.x releases, in order of the most recent release to the first release.

New Commands in DD OS 5.5.2

filesys option reset app-optimized-compression
Reset the Oracle Optimized Deduplication settings to none. Role required: admin.

filesys option set app-optimized-compression {none|oracle1}
Set Oracle Optimized Deduplication. Role required: admin.

Modified Output in DD OS 5.5.2

filesys encryption apply-changes
When an archive unit is offline and the DDFS is running, the system displays a message that encryption changes cannot be applied in an offline archive tier until it is brought back online and the file system is restarted.

filesys encryption abort-apply-changes
When an archive unit is offline and the DDFS is running, the system displays a message that the apply-changes request cannot be aborted for an offline archive unit until it is brought back online and the file system is restarted.

filesys encryption keys destroy
When an archive unit is offline and the DDFS is running, the system displays a message that this command does not destroy keys in an offline archive unit.

filesys encryption keys delete
When an archive unit is offline and the DDFS is running, the system displays a message that this command does not delete keys in an offline archive unit.

filesys encryption keys export
When an archive unit is offline and the DDFS is running, the system displays a message that this command cannot export keys for an offline archive unit.

filesys encryption keys show
When an archive unit is offline and the DDFS is running, the system displays a message that this command cannot display key information for an offline unit.

filesys encryption keys export
When an archive unit is offline and the DDFS is running, the system displays a message that this command cannot export keys for an offline archive unit.

New Commands in DD OS 5.5.1

filesys encryption keys show summary
Displays a usage summary for all keys in the system. If DD Extended Retention is enabled, information is displayed for both the active tier and the retention tier.

Modified Arguments in DD OS 5.5.1

filesys encryption keys delete
New arguments `[tier {active | archive } | archive-unit` *unit-name*`]`

filesys encryption keys destroy
New arguments `[tier {active | archive } | archive-unit` *unit-name*`]`

filesys encryption keys show
New arguments `[tier {active | archive } | archive-unit` *unit-name*`]`

Modified Output in DD OS 5.5.1

filesys archive unit add
If an offline archive unit exists, or one more archive units are configured, the system displays the following error message: "Cannot add more archive units to this system: The system already has one or more archive units."

filesys encryption embedded-key-manager show
Show both the running and configured key manager.

filesys encryption keys show
If DD Extended Retention is enabled, keys may be displayed for either or both the active tier and the retention tier.

filesys encryption show
Displays the configured key-manager if it is different from the currently running key-manager.

filesys encryption status
If DD Extended Retention is enabled, the status of apply-changes and re-encryption operations is displayed for both the active tier and the retention tier.

Modified Behavior in DD OS 5.5.1

filesys encryption abort-apply-changes
If DD Extended Retention is enabled, the apply-changes request is aborted for both the active tier and the retention tier.

filesys encryption apply-changes
If DD Extended Retention is enabled, the apply-changes request is posted for both the active tier and the retention tier.

filesys encryption keys delete
If DD Extended Retention is enabled, keys may be deleted for either or both the active tier and the retention tier.

filesys encryption keys destroy
If DD Extended Retention is enabled, keys may be destroyed for either or both the active tier and the retention tier.

filesys encryption keys export
If DD Extended Retention is enabled, keys are exported for both the active tier and the retention tier.

filesys encryption keys show
If DD Extended Retention is enabled, keys may be provided for either or both the active tier and the retention tier.

filesys encryption status
If DD Extended Retention is enabled, the status of apply-changes and re-encryption operations is provided for both the active tier and the retention tier.

New Commands in DD OS 5.5

filesys archive unit unseal
Unseals the last sealed retention unit and works only when there is no target unit; can be run only when the file system is offline.

filesys encryption abort-apply-changes
Aborts a previously issued apply-changes request.

filesys encryption status
Shows the status of apply-changes and re-encryption operations.

Modified Arguments in DD OS 5.5

filesys encryption keys delete
New argument `muid` *key-muid* (MUID is manufacturer unique identifier.)

filesys encryption keys destroy
New argument `muid` *key-muid* (MUID is manufacturer unique identifier.)

filesys encryption keys show
New argument `muid` *key-muid* (MUID is manufacturer unique identifier.)

filesys reset
Deleted argument`global-compression-type`

filesys set
Deleted argument`global-compression-type`

filesys show
Deleted argument`global-compression-type`

filesys show space
New arguments `[tier {active | archive | total} | archive-unit {all | unit-name}]`

Modified Output in DD OS 5.5

filesys clean status
Pre-analysis and analysis phases added; order and number of phases changed.

filesys clean watch
Pre-analysis and analysis phases added; order and number of phases changed.

filesys encryption keys destroy
MUID (manufacturer unique identifier) added.

filesys encryption keys export
`/ddr/var` directory changed to `/ddvar`.

filesys encryption keys show
MUID (manufacturer unique identifier) added.

filesys fastcopy
Two parameters indicating the direction of basefile tracking (source as base or destination as base) added. Tenants can fastcopy files only within the tenant-units they own (both source and destination).

filesys show compression
Footnote added: “This output is a historical record and represents compression achieved at the time of ingest. It is not the current space utilization. ”

filesys show space
Actual space utilization on a per retention unit basis reported, even for sealed and cleaning units.

Modified Behavior in DD OS 5.5

filesys archive unit expand
Allows expanding the size of a sealed unit.

filesys status
Adds tenant-admin and tenant-user to required roles.

Deleted Commands in DD OS 5.5

filesys option set global-compression-type

filesys option reset global-compression-type

filesys option show global-compression-type

filesys Guidelines and Restrictions

- In addition to admin permissions, command options for encryption require security officer authorization.

filesys archive

`filesys archive unit add`
Create a retention (archive) unit in the retention tier of the file system, change the state of disks or LUNs from Available to In Use, and add the new retention unit to the file system. Also view the list of retention unit sizes available in the retention tier. Role required: admin.

Note

If a system already has archive units configured, it will fail with the following error message: "Cannot add an archive unit to this system: The system already has an archive unit."

`filesys archive unit del` *`archive-unit`*
Delete a specific retention unit and change the state of disks or LUNs to available. A retention unit can be deleted from the tier only when the Data Domain system file system is disabled. Disabling the file system stops all Data Domain system operations, including `filesys clean`. Role required: admin.

This command destroys all data in the retention unit. Files within the retention unit must be deleted to remove them from the namespace.

Note

This command option is not available on a Retention Lock Compliance system.

`filesys archive unit expand` *`archive-unit`*
Expand the size of the specified retention unit and the size of a sealed unit. Role required: admin.

`filesys archive unit list {`*`archive-unit`* `| all}`
List all retention units or a specific retention unit. Role required: admin, user, backup-operator, security, none.

`filesys archive unit unseal [`*`archive-unit-name`*`]`
Unseals the last sealed unit and only works when there is no target unit. This command can only be run when the file system is offline. Role required: admin.

filesys clean

`filesys clean reset {schedule | throttle | all}`
Reset the clean schedule to the default of Tuesday at 6 a.m. (tue 0600), the default throttle of 50 percent, or both. Role required: admin.

`filesys clean set schedule { never | daily` *`time`* `| <day(s)>` *`time`* `| biweekly` *`day time`* `| monthly <day(s)>` *`time`* `}`

Set schedule for the clean operation to run automatically. Data Domain recommends running the clean operation once a week to maintain optimal availability of the file system. However, if there is no shortage of disk space you may clean less often. Role required: admin.

Argument Definitions

never
: Turn off the clean schedule.

daily
: Run command every day at the set time.

time
: Time is 24-hour format and must be specified by four digits. The time mon 0000 is midnight between Sunday night and Monday morning. 2400 is not a valid time. A new set schedule command cancels the previous setting.

biweekly
: Run command on alternate weeks. Bi-weekly cleaning is recommended for file migration on systems with Extended Retention.

monthly
: Starts command on the day or days specified at the set time. Days are entered as integers from 1 to 31.

day(s)
: Runs on the day or days specified. Days are entered as integers from 1 to 31.

Example 40

To run the clean operation automatically every Tuesday at 4 p.m.: **`# filesys clean set schedule tue 1600`**

Example 41

To set file system cleaning to run on alternate Tuesdays at 6:00 a.m., enter: **`# filesys clean set schedule biweekly "tue" "06:00"`**

Example 42

To run the operation more than once in a month, set multiple days in a single command. For example, to clean the file system on the first and fifteenth day of the month at 4 p.m., enter: **`# filesys clean set schedule monthly 1,15 1600`**

`filesys clean set throttle` *`percent`*

Set clean operations to use a lower level of system resources when the Data Domain system is busy. At zero percent, cleaning runs slowly or not at all, depending on how busy the system is. At 100 percent, cleaning uses system resources in the standard way. Default is 50 percent. When the Data Domain system is not running backup or restore operations, cleaning runs at 100 percent. Role required: admin.

Example 43

To set the clean operation to run at 30 percent of its potential speed: **`# filesys clean set throttle 30`**

`filesys clean show config`
Display settings for file system cleaning. All users may run this command option. Role required: admin, user, backup-operator, security, none.

`filesys clean show schedule`
Display current date and time for the clean schedule. All users may run this command option. Role required: admin, user, backup-operator, security, none.

`filesys clean show throttle`
Display throttle setting for cleaning. All users may run this command option. Role required: admin, user, backup-operator, security, none.

`filesys clean start`
Start clean process manually. When the process finishes, a message is sent to the system log citing the percentage of available storage space. Role required: admin.

`filesys clean status`
Display status of the clean process. Role required: admin.

`filesys clean stop`
Stop the clean process. Stopping the process means all progress is lost. Restarting the process means starting from the beginning. Role required: admin.

If the clean process slows down the system, run the `filesys clean set throttle` command to change the amount of system resources used by the clean process. Changes to system resource usage take effect immediately. Role required: admin.

`filesys clean watch`
Monitor the `filesys clean` process. Output of this command continuously updates as the `filesys clean` operation progresses. For example, output of verification phase shows the actual number of files moved to the target. Reporting concludes after the final phase. Role required: admin.

Press Ctrl-C to stop monitoring. Note the `filesys clean` process continues to run. All users may run this command.

Note

Because some files may be dropped during verification, output of the percent completion phase may not reach 100 percent. This is expected behavior.

filesys create

`filesys create`
Create a file system or associated RAID disk group with available and spare storage in the active tier. Change the state from Available to In Use. Role required: admin.

filesys destroy

`filesys destroy [and-zero]`
Delete all data in the Data Domain system file system including data configured with Retention Lock Governance, remove Replicator configuration settings, and return file system settings to defaults. When this process is finished, NFS clients connected to the Data Domain system may require a remount. Role required: admin.

Note

This command option is not available on a Retention Lock Compliance system.

By default, this command only marks the file system data as deleted. Disks are not overwritten with zeroes unless you specify the and-zero option. file system data marked deleted cannot be recovered, even if the disks have not been overwritten with zeroes. The `and-zero` option adds several hours to the destroy operation. It is not supported on Data Domain gateway systems.

filesys disable

`filesys disable`
Stop file system operations. Role required: admin.

filesys enable

`filesys enable`
Start the file system operations. On systems configured with Retention Lock Compliance, security officer authorization is required if there is time skew in the system clock. See the section on Retention Lock Compliance in the *EMC Data Domain Operating System Administration Guide* for details. Role required: admin.

filesys encryption

`filesys encryption abort-apply-changes`
Abort a previously issued apply-changes request. This applies to both the active and the retention tiers if DD Extended Retention is enabled. If an apply-changes operation is already in progress, the abort request will *not* abort the running operation, which will be allowed to finish. Role required: admin.

Note

If an archive unit is offline and file system is enabled, the system displays a warning that archive units are offline and that the abort-apply-changes operation will not be applied to these units.

`filesys encryption algorithm reset`
Reset the algorithm to the default (aes_256_cbc). After running this command, you must restart the file system with `filesys restart` for the change to take effect. Role required: admin.

`filesys encryption algorithm set {aes_128_cbc | aes_256_cbc | aes_128_gcm | aes_256_gcm}`
Select the encryption algorithm. The `aes_256_gcm` option (AES in the Galois/Counter mode) is the most secure algorithm, but is significantly slower than Cipher Block Chaining (CBC) mode. After running this command, you must restart the file system with `filesys restart` for the change to take effect. Role required: admin.

`filesys encryption algorithm show`
Display the encryption algorithm. Output indicates changes are pending, if applicable. Role required: admin, user, backup-operator, security, none.

`filesys encryption apply-changes`
Update the file system with the current encryption configuration. Encryption changes are applied to all data in the file system *active* tier during the next *cleaning cycle* and to the file system *retention* tier (if DD Extended Retention is enabled) during the next *space reclamation cycle*. Role required: admin.

Note

This process can take a long time to complete depending on the size of the data to be re-encrypted.

Note

If an archive unit is offline and file system is enabled, the system displays a warning that archive units are offline and that the apply-changes operation will not be applied to these units.

`filesys encryption disable`
Deactivate encryption. Disabling encryption means that new data does not get encrypted. You can then run `apply-changes` to decrypt the existing encrypted data. After running this command, you must restart the file system with `filesys restart` for the change to take effect. Role required: admin.

Note

This command requires security officer authorization. To enable run-time security officer authorization, login as a security officer, and then enter:

```
# authorization policy set security-officer enabled
```

`filesys encryption embedded-key-manager keys create`
Create a new key. An alert is raised when the new key is generated. You must run `filesys restart` for the key to be used to encrypt/decrypt any new data that is ingested. Role required: admin.

Note

This command requires security officer authorization. To enable run-time security officer authorization, login as a security officer, and then enter:

```
# authorization policy set security-officer enabled
```

`filesys encryption embedded-key-manager reset key-rotation-policy`
Reset key rotation policy of the embedded key manager. The `reset` command resets the key rotation policy to none. The new keys are not created automatically. Role required: admin.

Note

This command requires security officer authorization. To enable run-time security officer authorization, login as a security officer, and then enter:

```
# authorization policy set security-officer enabled
```

`filesys encryption embedded-key-manager set key-rotation-policy {`*`months`*` | none}`
Set the key rotation policy of the embedded key manager. The embedded key manager supports a maximum of 254 keys. The argument *months* is an integer between 1 and 12, which is the key rotation period. Each rotation creates a new key, which takes effect after the file system is restarted. If specifying *none*, the results are the same as those of

`filesys encryption embedded-key-manager reset key-rotation-policy`. Role required: admin.

Note

This command requires security officer authorization. To enable run-time security officer authorization, login as a security officer, and then enter:

```
# authorization policy set security-officer enabled
```

`filesys encryption embedded-key-manager show`
Show configuration of the embedded key manager. Role required: admin, user, backup-operator, security, none.

`filesys encryption enable`
Activate encryption for new data written to the file system. After running this command, you must restart the file system with `filesys restart` for the change to take effect. Role required: admin.

`filesys encryption key-manager disable`
Stops the Data Domain system from using the RSA DPM (Data Protection Manager) server for key management. (It will start using the embedded key manager after you run `filesys restart`.) The file system continues to use the latest Activated-RW key for encrypting the data. Role required: admin.

Note

This command requires security officer authorization. To enable run-time security officer authorization, login as a security officer, and then enter:

```
# authorization policy set security-officer enabled
```

`filesys encryption key-manager enable`
Enable key management. The RSA DPM (Data Protection Manager) key manager is available for external encryption key management. The local encryption key (which is the embedded key manager) administration method is also available. The RSA DPM key manager enables the use of multiple, rotating keys on a Data Domain system. RSA DPM supports a maximum of 254 keys. See the *EMC Data Domain Operating System Administration Guide* for additional information. Role required: admin.

`filesys encryption key-manager reset`
Clear the attributes of the key-manager. Role required: admin.

Note

This command requires security officer authorization. To enable run-time security officer authorization, login as a security officer, and then enter:

```
# authorization policy set security-officer enabled
```

`filesys encryption key-manager set {server` *`server-name`* `| port` *`port-number`* `| fips-mode {enabled | disabled} | key-class` *`key-class`* `| server` *`server-name`* `port` *`port-number`* `fips-mode {enabled | disabled} key-class` *`key-class`*`}`
Specify the attributes of the key-manager. For more details about configuring and setting up the RSA DPM server, see the *EMC Data Domain Operating System Administration Guide*. Role required: admin.

Note

RSA DPM (Data Protection Manager) supports the Key Class Cipher attributes Key Size, Algorithm, and Mode. Data Domain does not use the RSA DPM attributes Algorithm and Mode. These attributes are configured using `filesys encryption algorithm set {aes_128_cbc | aes_256_cbc | aes_128_gcm | aes_256_gcm}`. For Key Class, RSA DPM attribute "Get Key Behavior" has the choices "New Key Each Time" or "Use Current Key", however, Data Domain supports only "Use Current Key". When setting up a Key Class in RSA DPM for use in Data Domain, the Key Size must be 256 bits; otherwise the RSA DPM configuration will fail. An error message is not issued if the Key Class is incorrectly configured to generate a new key each time, but the Data Domain system will not receive the correct key to encrypt the data. For more details about configuring and setting up the RSA DPM server, see the *EMC Data Domain Operating System Administration Guide*.

`filesys encryption key-manager show`
Display details about the key manager. See the *EMC Data Domain Operating System Administration Guide* for descriptions of key states. Role required: admin, user, security none.

`filesys encryption keys delete {key-id | muid key-muid} [tier {active | archive} | archive-unit unit-name]`
Delete a specified encryption key from the file system, tier, or retention (archive) unit. Only a Destroyed-Compromised key or a Destroyed key can be deleted. A key can be deleted only if no data is currently encrypted with the key. By default, the key is deleted from entire system. Role required: admin.

Note

This command requires security officer authorization. To enable run-time security officer authorization, login as a security officer, and then enter:

```
# authorization policy set security-officer enabled
```

Note

If an archive unit is offline and file system is enabled, the system displays a warning that archive units are offline and that the encryption keys delete operation will not be applied to these units.

`filesys encryption keys destroy {key-id | muid key-umid} [tier {active | archive} | archive-unit unit-name]`
Mark a specified encryption key, from the file system, tier, or retention (archive) unit, to be destroyed. After an encryption key is destroyed, the system creates a flag for a re-encrypt operation and it is carried out the next time `filesys clean` runs. By default, the key is marked for destroy from the entire system. If DD Extended Retention is enabled, SREC (Space Reclamation) is responsible for re-encrypting data on the retention (archive) tier.

The key destroy operation simply flags a key to be destroyed, but it will not take effect right away because there is still data encrypted with it. There is no explicit re-encryption command; that job is scheduled when a key is marked to be in the compromised or destroyed state. Role required: admin.

Note

The re-encryption operation may start in the future and may take a long time depending on how much data needs to be re-encrypted. Use `filesys encryption status` to check the status.

Note

If an archive unit is offline and file system is enabled, the system displays a warning that archive units are offline and that the encryption keys destroy operation will not be applied to these units.

`filesys encryption keys export`
Export encryption keys. This applies to keys in both the active and the retention tiers if DD Extended Retention is enabled. All encryption keys in the file system are exported to a file that can recover encryption keys in the system if required. The key file is passphrase encrypted, and you will be prompted for a passphrase. To protect the key file, you may enter a new passphrase that differs from the Data Domain system passphrase. Lost or forgotten passphrases cannot be recovered. EMC recommends using this command when a new key is created or when a change of state occurs to any of the existing keys. EMC also recommends sending the exported file via FTP for storage in a secure location, accessible to authorized users only. Role required: admin.

Note

This command cannot export keys for an offline archive unit.

Note

This command requires security officer authorization. To enable run-time security officer authorization, login as a security officer, and then enter:

```
# authorization policy set security-officer enabled
```

`filesys encryption keys show [`*`key-id`*` | muid `*`key-muid`*`] [tier {active | archive} | archive-unit `*`unit-name`*`]`
Display information about encryption keys, from the file system, tier, or retention (archive) unit, including key id, key MUID, key state, and the amount of data encrypted with each key. Information about all keys in the system is displayed by default. Role required: admin.

Note

This command cannot display key information for an offline unit.

`filesys encryption keys show summary`
Display summary information for keys on the system. Information is displayed for both the active and the retention tiers if DD Extended Retention is enabled. Role required: admin, security.

Example 44 Example: Summary for system enabled with DD Extended Retention

```
# filesys encryption keys show summary
Key                                                                 Active Tier     Retention Tier
##   MUID                                                           post-comp size  post-comp size
--   ---------------------------------------------------------------  --------------  --------------
1    164                                                            0
2    7cf9acdbdc28cafe9693b06a7a45876c90663a62df64ef480a929f655030492e  0
```

Example 44 Example: Summary for system enabled with DD Extended Retention (continued)

```
3    a9f1571edbd4d6b1129c3267f47b03c46645229cdaf1186bd0fce60d17f3445e  72.00 MiB
--   ----------------------------------------------------------------  --------------  --------------
* Active Tier post-comp size is based on last cleaning of 2014/07/22 06:00:51.
* Retention Tier post-comp size is based on last space reclamation of 2014/07/22 06:00:51.
```

`filesys encryption keys sync`

Synchronize the key manager encryption keys. An alert is generated if a new key is detected. When the file system is restarted, the new key is used for reading and writing. Role required: admin.

Note

A Data Domain system retrieves a key from RSA DPM (Data Protection Manager) by Key Class. Choices for the RSA DPM attribute Get Key Behavior of a Key Class are “New Key Each Time” or “Use Current Key.” EMC Data Domain supports only the Key Class “Use Current Key”. An error message is not issued if the Key Class is incorrectly configured to generate a new key each time; however, the Data Domain system does not receive the correct key to encrypt the data.

`filesys encryption lock`

Note

Before locking the system, you must (1) verify that there are no keys in a compromised state, (2) perform a file system clean (`filesys clean`), and (3) disable the file system (`filesys disable`).

Lock the system by creating a new system passphrase and destroying the cached copy of the current passphrase. This command is useful when preparing a Data Domain system and its external storage devices for shipment. There is only one passphrase for each Data Domain system. After running this command, the system encryption keys are unrecoverable until the system is unlocked with the system passphrase. A new system passphrase is not stored and can be forgotten. It is recommended that you keep a record of the passphrase in a safe location. Data cannot be recovered without the new passphrase. Role required: admin.

Note

This command requires security officer authorization. To enable run-time security officer authorization, login as a security officer, and then enter:

```
# authorization policy set security-officer enabled
```

`filesys encryption show`

Check the status of the encryption feature. The system displays the configured key-manager if it is different than the currently running key-manager. Role required: admin, user, backup-operator, security, none.

Example 45 Example: Encryption enabled – no key-manager configured

```
# filesys encryption show
Encryption is enabled
The filesystem is unlocked
Algorithm: aes_256_cbc

Key manager in use:     Embedded Key Manager
```

Example 45 Example: Encryption enabled – no key-manager configured (continued)

```
Key rotation period:    not-configured
Last key rotation date: N/A
Next key rotation date: N/A
```

Example 46 Example: Key rotation policy set for embedded key manager

```
# filesys encryption show
Encryption is enabled
The filesystem is unlocked
Algorithm: aes_256_cbc

Key manager in use:     Embedded Key Manager
Key rotation period:    2 months
Last key rotation date: N/A
```

Example 47 Example: RSA DPM Key Manager configured and enabled

```
# filesys encryption show
Encryption is enabled
The file system is unlocked
Algorithm:              aes_256_cbc
Key manager in use:     RSA Key Manager
Server:                 dpmsrv1.mydomain.com
Port:                   443
Fips-mode:              enabled
Status:                 Online
Key-class:              TestKeyClass1
```

`filesys encryption status`

Display status of apply-changes and re-encryption operations. The status is displayed for both the active and the retention tiers if DD Extended Retention is enabled. The re-encryption operation is performed when a key is destroyed or marked as compromised, and the data encrypted with such a key needs to be encrypted with the current active key. The operation status can be *none* (no operation is needed), *pending*, *running* (in progress), or *done*. Role required: admin.

Example 48 Example: Status for system enabled with DD Extended Retention

```
# filesys encryption status
Active Tier:
    Apply-changes status: none
    Re-encryption status (for compromised or destroyed keys): none

Retention Tier:
    Retention unit: retention-unit-3
    Apply-changes status: none
    Re-encryption status (for compromised or destroyed keys): none
```

`filesys encryption unlock`

Unlock the file system. The system could be locked for several reasons: it is locked automatically after a headswap or chassis swap, or it could have been locked using `filesys encryption lock`. The system will prompt you for a passphrase. Role required: admin.

Note

This command requires security officer authorization. To log in as a security role, enter:

```
# authorization policy set security-officer enabled
```

Argument Definitions

fips-mode
Indicates whether the imported certificate for key management is FIPS (Federal Information Processing Standards) compliant. The default is `enabled`.

key-class
The key class configured on the RSA DPM (Data Protection Manager) server for the Data Domain system. The Key Class name must be enclosed in single or double quotes if the name contains special characters, such as a comma or a space.

key-id
The identifier for a specific key.

muid
The MUID (manufacturer unique identifier) for a specific key,

port
The port number of the RSA server on which the key manager is listening.

server
The name of the RSA DPM (Data Protection Manager) key manager server or IP address.

tier | archive-unit
For systems enabled with DD Extended Retention, the particular tier [active or retention (archive)] or retention (archive) unit.

filesys expand

`filesys expand`
Increase the filesystem by using all space in the active tier. Role required: admin.

filesys fastcopy

`filesys fastcopy source` *`src`* `destination` *`dest`*
Copy a file or directory tree from a Data Domain system source directory to another destination on the Data Domain system. Role required: admin, backup-operator, security.

Source names *src* that include spaces or special characters must be entered according to the following conventions.

- Enclose the entire source pathname with double quotation marks:

```
filesys fastcopy source "/data/col1/backup/.snapshot/fast copy"
destination /data/col1/backup/dir
```

OR

- Enter a backslash before the space. Do not add quotation marks:

```
filesys fastcopy source /data/col1/backup/.snapshot/fast\ copy
destination /data/col1/backup/dir2
```

Argument Definitions

source *src*
The location of the directory or file to copy. The first part of the path must be `/data/col1/`.

destination *dest*
The destination for the directory or file being copied. The first part of the path must be `/data/col1/`. If the destination already exists, you will be asked if you want to overwrite it.

filesys option

`filesys option disable report-replica-as-writable`
Set the reported read/write status of a replication destination file system to read-only. Use the `filesys disable` command before changing this option and use the `filesys enable` command after changing the option. Role required: admin.

With CIFS, use the `cifs disable` command before changing the option and use the `cifs enable` command after changing the option. Role required: admin.

`filesys option enable report-replica-as-writable`
Enable the filesys option. Role required: admin.

Set the reported read/write status of a replication destination file system to read/write. Use the `filesys disable` command before changing this option and use the `filesys enable` command after changing the option.

With CIFS, use the `cifs disable` command before changing the option and use the `cifs enable` command after changing the option.

`filesys option reset {local-compression-type | low-bw-optim | marker-type | report-replica-as-writable | staging-reserve | staging-clean | staging-delete-suspend | compute-segfeatures | app-optimized-compression}`
Return file system compression to the default settings on the destination Data Domain system. Role required: admin.

Argument Definitions

local-compression-type
Reset the compression algorithm to the default of lz.

low-bw-optim
This option is available only to authorized Data Domain and partner support personnel.

marker-type
Return the marker setting to the default of auto.

report-replica-as-writable
Reset the file system to read-only.

staging-clean
Staging-clean: Controls the automatic start of a cleaning operation after files have been deleted. Specify this as a percentage of the reserve. For example, if the staging reserve is 20% and staging-clean is 80%, then the system will start a cleaning operation when the space to be recovered from deleted files exceeds 16% of the total space. Default 0, range 0-200.

staging-delete-suspend
: Intended to prevent runaway deletions. For example, when no more reserve is available to increase available space and the client software keeps deleting files hoping to free up space. Specify as a percentage of the reserve. When the specified amount of space has been freed by deletions, the system allows no further deletions until after a clean is started. Default 0, range 0-400.

compute-segfeatures
: This option is available only to authorized Data Domain and partner support personnel.

staging-reserve
: Set staging reserve percentage from 0 to 90.

app-optimized-compression
: Reset the data-specific compression optimizations to none.

`filesys option set staging-reserve` *`percent`*

Reserve a percentage of total disk space for disk staging. Role required: admin.

```
filesys option show [local-compression-type | low-bw-optim |
marker-type | report-replica-as-writable | staging-reserve |
staging-clean | staging-delete-suspend | compute-segfeatures |
app-optimized-compression]
```

Show the file system option settings. By default, all file system options are displayed. To limit the output to a single system option, specify one of the system options. Role required: admin, user, backup-operator, security, none.

Argument Definitions

local-compression-type
: Display the current compression algorithm.

marker-type
: Display the current marker setting.

low-bw-optim
: This option is available only to authorized Data Domain and partner support personnel.

report-replica-as-writable
: Display the current reported setting on the destination Data Domain system.

staging-reserve
: Set staging reserve percentage from 0 to 90.

staging-clean
: This option is available only to authorized Data Domain and partner support personnel.

staging-delete-suspend
: This option is available only to authorized Data Domain and partner support personnel.

compute-segfeatures
: This option is available only to authorized Data Domain and partner support personnel.

app-optimized-compression
: Display which data-specific compression optimizations are enabled.

filesys restart

```
filesys restart
```

Disable and enable the filesystem in a single operation. Role required: admin, user, backup-operator.

filesys show

```
filesys show compression [filename] [recursive] [last n {hours
| days}] [no-sync]
```

```
filesys show compression [tier {active | archive}] summary |
daily | daily-detailed {[last n {hours | days | weeks |
months}] | start date [end date]
```

These command options displays the space used by, and compression achieved for, files and directories in the file system. When run on a Data Domain system with Extended Retention, information is also shown for the active or retention tiers. Values are reported in Gigibytes (GiB). See the *EMC Data Domain Operating System Administration Guide* for details. Role required: admin, user, backup-operator, security, none.

In general, the more often a backup procedure is run on a file or file system, the higher the compression. The output does not include global and local compression factors for the Currently Used table, but uses a dash instead. Output for a busy system may not return for several hours, depending on the number of files. Other factors may influence the output display.

Running the command without arguments generates default output that shows a summary of compression statistics for all files and directories in the file system for the last 7 days and the last 24 hours. Output includes details on active and retention tiers for systems with Extended Retention only.

Argument Definitions

recursive (Optional)
Display all files in all subdirectories as well as compression information for each file.

filename (Optional)
Synchronize all modified files to disk and then display compression statistics for the specified file or directory only. To display compression statistics for a specific file or directory without first synchronizing all modified files to disk, include the no-sync option.

Depending on the number of files in the file system, specifying a file name could cause this command to process for several hours before completing.

no-sync (Optional)
Use to not sync the file system prior to getting compression information.

tier {active | archive} (Optional)
Display results for the specified tier.

last *n* {hours | days | weeks | months} (Optional)
In the summary portion of the output, display file system compression statistics for the specified time frame instead of the past 7 days. The statistics for the last 24 hours remain in the summary output. If you specify a file or directory name, you cannot use this option with the weeks keyword or the months keyword.

summary (Optional)
Display all compression statistics, summarized in the following categories:

- Storage currently used.
- Data written in the last 7 days. By including the `last` *n* option or the `start` *date* option, you can display statistics for a different time frame.
- Data written in the last 24 hours.

daily (Optional)
In addition to the summary output, display the following information for each day, over the previous four full weeks, plus the current partial week. This option is not available if you specify a file or directory name.

daily-detailed (Optional)
Display the daily output, but also include the following information for each day. This option is not available if you specify a file or directory name.

start *date* (Optional)
In the summary portion of the output, display file system compression statistics for the time frame that begins on the specified day instead of the past 7 days. The statistics for the last 24 hours remain in the summary output. If you specify a time frame less than the previous 4 weeks, plus the current full week, the daily or daily-detailed output (if specified) is truncated to the shorter time frame.

Specify *date* using the format *yyyy-mm-dd*. By default, the last day of the time frame specified with this argument is the most recent, full day elapsed.

end *date* (Optional)
Valid only if the start option is used. In the summary portion of the output, display file system compression statistics for the time frame that ends on the specified day. In general, the more often a backup is done for a particular file or file system, the higher the compression. On a busy system, this process may not complete for several hours, depending on the number of files. Other factors may also affect results.

On a standard Data Domain system, output includes information on active tier only.

Output Definitions

Pre-Comp
Data written before compression.

Post-Comp
Storage used after compression.

Global-Comp Factor
Ratio of Pre-Comp / (size after global compression). Not applicable to the storage currently used.

Local-Comp Factor
Ratio of (size after global compression)/Post-Comp. Not applicable to the storage currently used.

Total-Comp Factor
Ratio of Pre-Comp / Post-Comp.

Reduction %
Percentage value (Pre-Comp - Post-Comp) / Pre-Comp) * 100. This is the default output format.

Example 49

`filesys show compression` *`filename`* `[recursive]`

Displays all files in all subdirectories and prints compression information for each file as well as the summary for *filename*.

`filesys show file-info` *`filename`*

Display detailed information about the specified file. Specify the fully qualified path to the file. Role required: admin.

`filesys show space [tier {active | archive | total} | archive-unit {all | unit-name}]`

Displays the space available to and used by file system resources, including per-unit space usage statistics for sealed and cleaning archive units. Values are reported in gigibytes (GiB). Role required: admin, user, backup-operator, security, none. Output includes:

- If the tier option is specified, the system shows a summary for the entire tier.
- If archive-unit option is specified, the system shows space usage for each unit.
- If none is specified, the system shows summary tables for the active tier, archive, and total.
- The total option is valid only for systems with Extended Retention and, if total is used, the system displays a summary of both active and archive tiers.

Note

Keywords tier and archive-unit are mutually exclusive. The user can only specify one or the other but not both.

Output Definitions

Size GiB
Total storage capacity of a file system resource.

Used GiB
Amount of data stored on a file system resource.

Avail GiB
Amount of free space on a file system resource.

Use%
Ratio of data stored to total capacity, multiplied by 100.

Cleanable GiB
Estimated amount of recoverable free space. Command output displays space availability and usage information for the following file system components:

/data: pre-comp
Amount of virtual data stored on the Data Domain system. Virtual data is the amount of data sent to the Data Domain system from backup servers.

/data: post-comp
Amount of total physical disk space available for data, actual physical space used for compressed data, and physical space still available for data storage. Warning messages go to the system log and an email alert is generated when the Use% figure reaches 90%, 95%, and 100%. At 100%, the Data Domain system stops accepting data from backup servers.

/ddvar
: Approximate amount of space used by and available to the log and core files. Use this directory to free space in this area, remove old logs and core files. You can also delete core files from the /ddvar/core directory or the /ddvar/ext directory if it exists.

  The total amount of space available for data storage can change because an internal index may expand as the Data Domain system fills with data. The index expansion takes space from the Avail GiB amount.

  If Use% is always high, use the command option `filesys clean show-schedule` to see how often the cleaning operation is scheduled to run automatically. Use `filesys clean schedule` to run the operation more often.

`filesys show uptime`
Display the amount of time passed since the file system was last enabled. The display is in days, hours, and minutes. Role required: admin, user, backup-operator, security, none.

filesys status

`filesys status`
Display the state of the filesystem process. If the filesystem was shut down with a Data Domain system command, such as filesys disable, the output display includes the command name in square brackets. Role required: admin, user, backup-operator, tenant-admin, tenant-user, security, none.

filesys sync

`filesys sync`
Synchronize modified files to disk. Role required: admin, backup-operator, security.

CHAPTER 14

help

The Command Line Interface (CLI) displays two types of help, syntax-only help and command-description help that includes the command syntax.

The following guidelines describe how to use syntax-only help.

- To list the top-level CLI commands, enter a question mark (**?**), or type the command `help` at the prompt.
- To list all forms of a top-level command, enter the command with no options at the prompt or enter *command* `?`.
- To list all commands that use a specific keyword, enter `help` *keyword* or `?` *keyword*. For example, `? password` displays all Data Domain system commands that use the password argument.

The following guidelines describe how to use command-description help.

- To list the top-level CLI commands, enter a question mark (**?**), or type the command `help` at the prompt.
- To list all forms of a top-level command with an introduction, enter `help` *command* or `?` *command*.
- The end of each help description is marked `END`. Press Enter to return to the CLI prompt.
- When the complete help description does not fit in the display, the colon prompt (:) appears at the bottom of the display. The following guidelines describe what you can do when this prompt appears.
  - To move through the help display, use the up and down arrow keys.
  - To quit the current help display and return to the CLI prompt, press **q**.
  - To display help for navigating the help display, press **h**.
  - To search for text in the help display, enter a slash character (**/**) followed by a pattern to use as search criteria and press Enter. Matches are highlighted.

CHAPTER 15

ipmi

The `ipmi` command monitors and manages a Data Domain system deployed remotely. Command options enable administrators to monitor remote systems and to power the systems on or off as required. The Serial-Over-LAN (SOL) feature is used to view the serial output of a remote system boot sequence. For more information, including the list of supported models, see the *EMC Data Domain Operating System Offline Diagnostics Suite User's Guide*.

This chapter contains the following topics:

ipmi Change History

There have been no changes to this command since the 5.4 release.

ipmi Guidelines and Restrictions

- Users cannot log in to IPMI via SSH. See the *EMC Data Domain Operating System Administration Guide* for instructions on managing remote systems.
- IPMI (on/off/cycle/status) and SOL are not supported on models DD140, DD610, DD630, and DD2500.

ipmi config

`ipmi config` *`port`* `{dhcp | ipaddress` *`ipaddr`* `netmask` *`mask`* `gateway` *`ipaddr`*`}`

Configure the IPMI static or dynamic IP address of a BMC-capable interface. If configuring a static IP, you must provide the BMC IP address, netmask, and gateway address. See the *EMC Data Domain Operating System Administration Guide* for details. Role required: admin.

Note

If the IPMI port also supports IP traffic (for administrator access or backup traffic), the interface port must be enabled with the `net enable` command before you configure IPMI.

ipmi disable

`ipmi disable {`*`port`* `| all}`

Disable IPMI remote access to a single system, or all systems. Role required: admin.

ipmi enable

`ipmi enable {`*`port`* `| all}`

Enable IPMI remote access to a single system, or to all systems. Role required: admin.

ipmi remote

`ipmi remote console ipmi-target {`*`ipaddr`* `|` *`hostname`*`} user` *`user`*

Activates the Serial-Over-Lan (SOL) feature, which enables viewing text-based serial output of a remote Data Domain system without a serial server. SOL is used in combination with the remote power cycle command to view the remote system's boot sequence. For more information, see the *EMC Data Domain Operating System Administration Guide*. Role required: admin.

`ipmi remote power {on | off | cycle | status} ipmi-target {`*`ipaddr`* `|` *`hostname`*`} user` *`user`*

Power on, power off, or power cycle a remote target system from an initiator system. Role required: admin.

ipmi reset

`ipmi reset`
Reset LAN and SOL configuration and clear all IPMI users. Role required: admin.

ipmi show

`ipmi show config`
View the configuration of local IPMI interfaces. Output includes the dynamic or static IP address, gateway, netmask, and MAC address. Role required: admin.

`ipmi show hardware`
View the port names and firmware version of the local BMC. Output also includes the IPMI version, manufacturer, MAC addresses. The Link Status column shows if the LAN cable is connected to the LAN-IPMI shared port.

Link status cannot be determined on Data Domain systems with a dedicated IPMI port. These include models DD640, DD4200, DD4500, and DD7200. Role required: admin.

ipmi user

`ipmi user add` *`user`*
Add new IPMI user. Role required: admin.

Note

User root is not supported for IPMI connections on DD160, DD880, and DD880G systems.

`ipmi user change` *`user`*
Change the password of an IPMI user. Role required: admin.

`ipmi user del` *`user`*
Delete an IPMI user. Role required: admin.

`ipmi user list`
View a list of IPMI users, including names, IDs, and permissions. Role required: admin.

`ipmi user reset`
Clear all IPMI users. If this is the first time using IPMI, we recommend running this command to clear IPMI users who may be out of synch between two ports, and to disable default users. Role required: admin.

CHAPTER 16

license

The `license` command adds, deletes, and resets keys for licensed features and storage capacity.

This chapter contains the following topics:

license Change History

There have been no changes to this command since the 5.4 release.

license Guidelines and Restrictions

- License codes are case-insensitive. Include the hyphens when entering codes.
- The following software options require separate licenses. See the EMC Online Support site for details.
  - DD Boost
  - Extended Retention (formerly “Archiver”)
  - Encryption
  - Expanded Storage
  - I/OS
  - Replication
  - Retention Lock Compliance
  - Retention Lock Governance
  - Shelf Capacity
  - Virtual Tape Library (VTL)

license add

`license add` *`license-code`* [*`license-code`* `...`]

Add one or more licenses for features and storage capacity. Include dashes when entering the license code. Role required: admin.

license delete

`license del` *`license-feature`* [*`license-feature`* `...`] | *`license-code`* [*`license-code`* `...`]

Delete one or more licenses for features or storage capacity. Role required: admin. Security officer authorization is required to delete Retention Lock Compliance licenses.

license reset

`license reset`

Remove all licenses. Role required: admin. Security officer authorization is required to delete Retention Lock Compliance licenses.

license show

`license show [local]`

View license keys and features. If the `local` argument is included in the option, output includes details on local node only. Role required: admin.

CHAPTER 17

log

The `log` command manages and displays the Data Domain system log file. Messages from the alerts feature, the autosupport reports, and general system messages are sent to the `log` directory (`/ddvar/log`). A log entry appears for each Data Domain system command given on the system.

Data Domain systems can send network log messages to other systems enabled to listen. The Data Domain system sends the log in the standard syslog format. When remote logging is enabled, all messages in the messages and `kern.info` files are exported.

Message selectors include:

***.notice**
Send all messages at the notice priority and higher.

***.alert**
Send all messages at the alert priority and higher (alerts are included in *.notice).

kern.*
Send all kernel messages (`kern.info` log files).

local7.*
Send all messages from system startups (`boot.log` files).

See the vendor-supplied documentation for details on managing the selectors and receiving messages on a third-party system.

This chapter contains the following topics:

log Change History

There have been no changes to this command since the 5.4 release.

log host

`log host add` *host*

Add a system (remote log host) to the list that receives Data Domain system log messages. Role required: admin.

Note

If using three or more remote log hosts, they must be added by entering the IP address in the *host* argument instead of the host name.

`log host del` *host*

Remove a system from the list of systems that receive Data Domain system log messages. Role required: admin.

`log host disable`

Disable sending log messages to other systems. Role required: admin.

`log host enable`

Enable sending log messages to other systems. Role required: admin.

`log host reset`

Reset the log sending feature to the defaults of disabled and an empty list. Role required: admin.

`log host show`

Display the list of systems that receive log messages and are in the state of enabled or disabled. Role required: admin, security, user, backup-operator, or none.

log list

`log list`

List the files in the log directory with the date each file was last modified and the size of each file. For information on the log files, see the *EMC Data Domain Operating System Administration Guide*. Role required: admin, security, user, backup-operator, or none.

log view

`log view [`*filename*`]`

View the log files. When viewing the log, use the up and down arrows to scroll through the file. Use the q key to quit. Enter a forward slash to search forward or a question mark to search backward for a pattern such as a date. If filename is not included, the command displays the current messages file. Role required: admin, security, user, backup-operator, or none.

log watch

`log watch [`*filename*`]`

View new message entries as they occur. Use Ctrl-C to stop the display. If a filename is not included, the command displays the current messages file. Role required: admin, security, user, backup-operator, or none.

log

CHAPTER 18

migration

The `migration` command copies all data from one Data Domain system to another. Use this command when upgrading to a larger capacity Data Domain system. Migration is typically performed in a LAN environment.

Migration may also be used to copy replication configurations, known as “contexts.” See the *EMC Data Domain Operating System Administration Guide* for instructions.

This chapter contains the following topics:

migration Change History

There have been no changes to this command since the 5.4 release.

migration Guidelines and Restrictions

- All data under `/backup` is migrated and exists on both systems after migration.
- After migrating replication contexts, the contexts remain on the source. You must break replication contexts on the migration source after the process is completed.
- For best results, avoid backup operations to a migration source during a migration operation.
- A migration destination does not require a replication license or encryption license unless the source system is licensed for those software options.
- With the exception of collection replication, the migration destination must have equal or larger capacity than the used space on the migration source.
- The migration destination must have an empty file system.
- Any setting of the system's replication throttle also applies to migration. If the migration source has throttle settings, use `replication throttle set override` to set the throttle to the maximum (unlimited) before starting migration.
- The procedure for migrating from an encryption-enabled source requires additional steps.

migration abort

`migration abort`

Stop a migration process and return the Data Domain system to its previous state.

If the migration source is part of a replication pair, replication is restarted. You must run `migration abort` on both the migration source and the destination system. And after you run `migration abort` on a destination system, you must run `filesys destroy` on the destination system before the file system can be reenabled. Be aware that, after running `migration abort`, the password on the destination system will be the same as the password on the migration source.

Role required: admin.

migration commit

`migration commit`

Limit migration to data received by the source at the time the command is entered. You can enter `migration commit` and limit the migration of new data any time after entering `migration send`. After `migration commit`, all data on the source Data Domain system, including new data for contexts migrated to the destination, is sent only to the destination.

Write access to the source is blocked after you enter `migration commit` and during the time required to complete migration. After the migration process is finished, the source is opened for write access, but new data is not migrated to the destination.

Role required: admin.

migration receive

`migration receive source-host` *`src-hostname`*
Prepare a Data Domain system to be a migration destination. When preparing the destination, do not run `filesys enable`.

Run `migration receive` under the following conditions:

- On the migration destination only.
- Before entering `migration send` on the migration source.
- After running `filesys destroy` and `filesys create` on the destination.

Role required: admin.

Example 50

To prepare a destination for migration from the source hostA:

```
# filesys destroy
# filesys create
# migration receive source-host hostA
```

migration send

`migration send {`*`obj-spec-list`* `| all} destination-host` *`dst-hostname`*
Start migration.

Use `migration send` under the following conditions:

- Only on the migration source.
- Only when no backup data is being sent to the migration source.
- After running `migration receive` on the destination.

The *obj-spec-list* is `/backup` for systems that do not have a replication license. With replication, this argument represents one or more contexts from the migration source. After you migrate a context, all data from the context remains on the source system, but the context configuration is moved to the migration destination.

A context in the *obj-spec-list* can be:

- The destination string, as defined when setting up replication, for example:

```
dir://hostB/backup/dir2col://hostBpool://hostB/pool2
```

- The context number, such as `rctx://2`, as shown in the output from `replication status`.
- The keyword `all`, which migrates all contexts from the migration source to the destination.

New data written to the source is marked for migration until you run `migration commit`. New data written to the source after `migration commit` is not migrated. Note that write access to the source is blocked from the time you run `migration commit` until the migration process concludes.

Running `migration send` will continue until you run `migration commit`. Run `migration commit` on the migration source first, and then on the destination.

Note

After you run `migration send`, the migration source remains in read-only mode until all contexts are synchronized. To avoid the time spent in this mode, it is recommended that you synchronize the replication contexts before running `migration send`. Run `replication sync` to synchronize replication contexts. Run `migration send` immediately after the synchronization process concludes.

With the exception of licenses and key-manager settings, all data on the migration source is always migrated, even when a single directory replication context is specified.

Role required: admin.

Example 51

To start migration of data only (excluding replication contexts, even if replication contexts are configured) to a migration destination named hostC:

```
# migration send /backup destination-host hostC
```

Example 52

To start a migration that includes a collection replication context (replication destination string) of col://hostB:

```
# migration send col://hostB destination-host hostC
```

Example 53

To start migration with a directory replication context of `dir://hostB/backup/dir2`:

```
# migration send dir://hostB/backup/dir2 destination-host hostC
```

Example 54

To start migration with two replication contexts using context numbers 2 and 3:

```
# migration send rctx://2 rctx://3 destination-host hostC
```

Example 55

To migrate all replication contexts:

```
# migration send all destination-host hostC
```

migration show stats

`migration show stats`

Display migration statistics during the migration process.

Role required: admin.

Output Definitions

Bytes Sent
The total number of bytes sent from the migration source. This value includes backup data, overhead, and network overhead. On the destination, this value includes overhead and network overhead. Use this value (and the next value, **Bytes Received**) to estimate network traffic generated by migration.

Bytes Received
The total number of bytes received at the destination. On the destination, this value includes data, overhead, and network overhead. On the source, this value includes overhead and network overhead. Use this value (and the previous value, **Bytes Sent**) to estimate network traffic generated by migration.

Received Time
The date and time at which the most recent records were received.

Processed Time
The date and time at which the most recent records were processed.

migration status

`migration status`

Display the status of migration at the time the command is run.

Role required: admin.

migration watch

`migration watch`

Track the initial phase of migration (when write access is blocked). The command output shows the percentage of the migration process that has been completed.

Role required: admin.

Examples

Preparing for Migration

If a migration source has encryption enabled, you must perform the following tasks on the destination before starting the migration process.

Procedure

1. Add the encryption license.
   ```
   # license add license-code
   ```
2. Enable encryption. This command prompts you for a passphrase. Use the same passphrase as the migration source.
   ```
   # filesys encryption enable
   ```

3. Restart the file system.

```
# filesys restart
```

After you finish

If the migration source has DPM key manager configured and enabled, clear the DPM attributes on the destination.

```
# filesys disable
# filesys encryption key-manager reset
# filesys restart
```

After migration concludes, configure the DPM attributes on the destination to be the same as the DPM attributes on the migration source, and then enable the DPM key manager.

See the `filesys` commands for more information.

Migrating Data (Does Not Apply to Replication Contexts)

To migrate data from hostA, to a destination, hostB:

Procedure

1. On hostB (the destination), enter:

```
# filesys disable
# filesys destroy
# filesys create
# migration receive source-host hostA
```

2. On hostA (the source), enter:

```
# migration send /backup destination-host hostB
```

3. On either host, enter:

```
# migration watch
```

4. At the appropriate time for your site, create a migration end point. Note that three phases of migration may take many hours. During that time, new data sent to the source is also marked for migration.
5. After the three migration phases are finished, enter the following command on hostA first, and then on the destination, hostB:

```
# migration commit
```

Migrating Data and a Context

To migrate data and a context from a source, hostA, to a destination, hostC, when hostA is also a directory replication source for hostB.

Procedure

1. On hostC (the migration destination), enter:

```
# filesys disable
# filesys destroy
# filesys create
# migration receive source-host hostA
```

2. On hostA (the migration and replication source), enter:

```
# migration send dir://hostB/backup/dir2 destination-host hostC
```

   Note that this command also disables the file system.

3. On the source migration host, enter:

```
# migration watch
```

4. First on hostA and then on hostC, enter:

```
# migration commit
```

   Note that this command also disables the file system.

5. On hostB (the replication destination), enter the following command options to change the replication source to hostC:

```
# filesys disable
# replication modify dir://hostB/backup/dir2
  source-host hostC
# filesys enable
```

CHAPTER 19

mtree

The `mtree` command enables operations on a single “managed tree” (MTree) of a filesystem. An MTree is a logical partition of the namespace in the file system that can group together a set of files for management purposes; for example, snapshot schedules, replication, or retention locking.

This chapter contains the following topics:

MTree Change History

This section provides a list of changes since the 5.4 release, for all 5.5.x releases, in order of the most recent release to the first release.

New Commands in DD OS 5.5.2.0

mtree option reset app-optimized-compression mtree *mtree_path*
Reset the Oracle Optimized Deduplication setting on the specified MTree to its default value, none.

mtree option set app-optimized-compression {none | global | oracle1} mtree *mtree_path*
Set Oracle Optimized Deduplication on the specified MTree.

New Commands in DD OS 5.5.1

mtree option show *mtree_path*
Displays option values for the MTree found at the *mtree_path*.

New Commands in DD OS 5.5

mtree modify
Associates an MTree with a tenant-unit.

mtree retention-lock report generate retention-details mtrees
List all retention-lock files in an MTree and their expiration times.

mtree show performance
Outputs MTree performance using the following columns: Date, Time, Throughput (read and write), Streams (rd/wr/r+/w+/). Data written via replication is not included in the output.

Modified Arguments in DD OS 5.5

mtree create
Modified to use `tenant-unit`.

mtree modify
Changed output of `mtree modify` *mtree-path* tenant-unit {*tenant-unit* | `none`} so that the command **mtree modify /data/col1/mtree1 tenant-unit google** results in the MTree `/data/col1/mtree1` being assigned to tenant-unit “google”.

mtree list
The `tenant-unit` argument was added.

mtree show compression
The `tenant-unit` argument was added.

Modified Output in DD OS 5.5

mtree create
Modified to display `tenant-unit`.

mtree delete
The output now includes a warning before the system deletes an MTree if the MTree belongs to a tenant-unit.

mtree list

When Secure Multi-tenancy (SMT) is not enabled, the system displays three columns: Name, Pre-Comp (GiB), and Status. When SMT is enabled, the system also displays Tenant Unit.

mtree show compression

Output has been modified to clarify the semantics of the command by inserting the following footnote: This output is a historical record and represents compression achieved at the time of ingest. It is not the current space utilization.

mtree Guidelines and Restrictions

- A single controller supports a maximum of 100 MTrees; however, system performance may degrade if the number of MTrees simultaneously engaged in read or write streams exceeds 14. For best results, limit the number of active MTrees to 14, and, when possible, consolidate operations on the same MTree into one operation.
- MTrees cannot be created if the maximum of 100 has been reached or if there is no available space.
- MTree quotas cannot be set on the `/data/col1/backup` directory.
- The maximum quota value is 4096 PiB.
- Quota limits are pre-compressed values.
- The default setting for MTree quota limits is disabled.
- MTree quota limits are set for the active tier only when set on a Data Domain system with Extended Retention.

mtree create

`mtree create` *`mtree-path`* `[tenant-unit` *`tenant-unit`*`] [quota-soft-limit` *`n`* `{MiB|GiB|TiB|PiB}] [quota-hard-limit` *`n`* `{MiB|GiB|TiB|PiB}]`

Create an MTree under the specified path. The format of the *mtree-path* is `/data/col1/`*mtree-name*. An error message notifies you to enter a different name if another MTree with the same name exists. Role required: admin.

Naming conventions for creating MTrees include uppercase and lowercase letters (A-Z, a-z), numbers 0-9, single, non-leading embedded space, exclamation point, hash, dollar sign, ampersand, caret, tilde, left and right parentheses, left and right brackets, left and right braces.

If no quota option is specified, the default is unlimited for both soft and hard limits, meaning there are no quota limits.

When setting quota limits, a warning appears if the new limit is lower than the current space usage of the MTree. The command does not fail, but subsequent writes to the MTree are rejected. An error message appears if you are setting a soft limit that is greater than or equal to the hard limit. When the hard limit is reached for an MTree quota, write operations stop and no more data can be written to the MTree. Data can be deleted.

Argument Definitions

mtree-path

Displays MTrees under a specified path only.

tenant-unit (Optional)
The basic unit of a multi-tenancy configuration. A tenant unit is a secure, isolated partition for tenant-specific data and control flow within a Data Domain system.

Example 56

To create MTree `/data/col1/backup1` with no quota limits:

```
# mtree create /data/col1/backup1
```

Example 57

To set a soft limit quota of 10 GiB on MTree `/data/col1/backup1`:

```
# mtree create /data/col1/backup1 quota-soft-limit 10 GiB
```

Example 58

To set a hard limit quota of 10 TiB on MTree `/data/col1/backup2`:

```
# mtree create /data/col1/backup2 quota-hard-limit 10 TiB
```

Example 59

To set a tenant-unit on `/data/col1/backup3`:

```
# mtree create /data/col1/backup3 tenant-unit tenant1
```

mtree delete

`mtree delete` *`mtree-path`*

Delete the specified MTree (denoted by the pathname). MTrees marked for deletion remain in the file system until the `filesys clean` command is run. This command option is not allowed on Retention Lock Governance or Retention Lock Compliance MTrees unless they are empty. You can revert the marked-for-deletion state of that MTree by running the `mtree undelete` command. See the *EMC Data Domain Operating System Administration Guide* for details on Retention Lock Compliance and Governance. Role required: admin.

Effects of deleting an MTree include:

- The MTree appears in the output of the `mtree list` command option and is marked with the status value D.
- File service to a deleted MTree is rejected. Deleted MTrees are not visible through NFS or CIFS clients.
- When an MTree is removed from the file system, snapshots associated with that MTree are also deleted from the `/data/col1/`*`mtree-name`*`/.snapshot/` directory.

mtree list

`mtree list [`*`mtree-path`*`] [tenant-unit `*`tenant-unit`*`]`

Display the list of MTrees. When Secure Multi-tenancy (SMT) is not enabled, the system displays three columns: Name, Pre-Comp (GiB), and Status. When SMT is enabled, the system also displays Tenant Unit. Role required: admin, user, backup-operator, tenant-admin, tenant-user, security, none.

Argument Definitions

***mtree-path* (Optional)**
Display MTrees under the specified path only. This command supports the asterisk (*) wildcard character in the MTree pathname. Values include:

- `/data/col1/mtree1`
- `/data/col1/mtree*`
- `*mtree*`

tenant-unit (Optional)
The basic unit of a multi-tenancy configuration. A tenant unit is a secure, isolated partition for tenant-specific data and control flow within a Data Domain system.

Output Definitions

When SMT is enabled, tenant-unit will be displayed if it is configured. If it is not configured, the system will display "-". Output includes the MTree pathname, pre-compression, and status. Status is based on pre-defined values:

D
Marked for deletion. MTree will be removed from the file system by the filesys clean command. Can be unmarked for deletion by using the mtree undelete command only if the filesys clean command has not been run.

Q
Quota defined.

RO
Read-only access.

RW
Read/write access.

RD
Replication destination.

RLCE
Retention Lock Compliance enabled.

RLGE
Retention Lock Governance enabled.

RLGD
Retention Lock Governance disabled.

mtree modify

`mtree modify` *`mtree-path`* `tenant-unit` *`tenant-unit`* `|` *`none`*

Assign an MTree to a tenant-unit. Role required: admin.

Argument Definitions

mtree-path
Display MTrees under the specified path only.

none
Use *none* to remove a tenant-unit associated with the mtree.

tenant-unit (Optional)
The basic unit of a multi-tenancy configuration. A tenant unit is a secure, isolated partition for tenant-specific data and control flow within a Data Domain system.

mtree option

`mtree option reset app-optimized-compression mtree` *`mtree_path`*
Reset the Oracle Optimized Deduplication setting on the specified MTree to its default value, none.

`mtree option set app-optimized-compression {none | global | oracle1} mtree` *`mtree_path`*
Set Oracle Optimized Deduplication on the specified MTree.

Argument Definitions

none
Oracle Optimized Deduplication is disabled.

global
The MTree uses the system-level app-optimized-compression value (none or oracle).

oracle1
Oracle Optimized Deduplication is enabled.

`mtree option show [mtree` *`mtree_path`*`]`
Display option values for the MTree found at the *mtree_path*. If no MTree is specified, the system displays option values for all MTrees.

Argument Definitions

mtree_path
The full path of the MTree in the file system.

mtree rename

`mtree rename` *`mtree-path new-mtree-path`*
Rename the specified MTree. Note that `/data/col1/backup` cannot be renamed. Retention Lock Governance or Retention Lock Compliance MTrees can only be renamed if they are empty. Role required: admin.

This command option requires security officer authorization if Retention Lock Compliance is enabled on the specified MTree.

mtree retention-lock

`mtree retention-lock disable mtree` *`mtree-path`*
Disable Retention Lock for the specified MTree. This command option is allowed on Retention Lock Governance MTrees only. It is not allowed on Retention Lock Compliance MTrees. See the *EMC Data Domain Operating System Administrator's Guide* for details on Retention Lock Compliance and Governance. Role required: admin.

`mtree retention-lock enable mode` *`{compliance | governance}`*
`mtree mtree-path`
Enable Retention Lock for the specified MTree. Use the compliance argument to meet the strictest data permanence regulatory standards, such as those of SEC17a-4f. Enabling Retention Lock Compliance requires security officer authorization. Role required: admin.

Use the governance argument to propagate the same protection provided in the previous release of DD OS. The level of security protection is lower than Retention Lock Compliance.

When Retention Lock is enabled on an MTree, any file in the MTree may become locked by setting its *atime* to the future. Additionally, renaming a non-empty directory in the MTree is disabled. See the *EMC Data Domain Operating System Administration Guide* for details on Retention Lock Compliance and Governance, and for instructions on setting retention time.

To enable Retention Lock Compliance on an MTree, enter: **`# mtree retention-lock enable mode compliance mtree /data/col1/mtree_name`**

Note that `/data/col1/backup` cannot be configured for Retention Lock Compliance.

`mtree retention-lock reset {min-retention-period | max-retention-period} mtree` *`mtree-path`*
Reset the minimum or maximum retention period for the specified MTree to its default value. The command option is allowed on MTrees with Retention Lock Governance enabled. Role required: admin.

See the *EMC Data Domain Operating System Administration Guide* for details on Retention Lock Compliance and Governance and for instructions on setting retention time.

`mtree retention-lock report generate retention-details mtrees {`*`mtree-list`* `| all} [format {text | tsv | csv}] [output-file` *`filename`*`]`
Lists all retention-lock files in one or multiple mtrees, their expiration time, mode of retention, and size. If the output-file *filename* option is specified, then the report will be written to /ddvar/log/debug/retention-lock-reports/*filename*; otherwise, the report will go to standard output. The report includes a timestamp indicating the time it was generated. The default output format is text. If the file already exists, an error is generated. Role required: admin.

`mtree retention-lock revert` *`path`*
Revert all Retention Lock files in a specified path to non-Retention Lock files. Note that directories and files within Retention Lock Compliance Mtrees cannot be reverted. Role required: admin.

The base of the path must be `/data/col1/`*`mtree-name`*`/` or `data/col1/backup/`.

Reverting Retention Lock Governance generates a Data Domain system alert (at the `Alert` severity level) and logs the names of the reset files. Data Domain recommends when a recipient receives the alert, he or she confirms the reset operation was intended.

`mtree retention-lock set {min-retention-period | max-retention-period}` *`period`* `mtree` *`mtree-path`*
Set the minimum or maximum retention period for the specified MTree. This command option requires security officer authorization if Retention Lock Compliance is enabled on the MTree. Role required: admin.

Users cannot set the minimum retention period to fewer than 12 hours. Doing so generates a message notifying the user that the entry was invalid and stating the minimum retention period allowed.

When setting the lock period for Retention Lock Compliance MTrees, users cannot set the period to be less than the current minimum or maximum period allowed. Doing so generates a message notifying the user that the entry was invalid and stating the minimum or maximum retention period allowed.

The retention period is specified in the format [number] [unit]. Possible unit values are:

- min

- hr
- day
- mo
- year

The retention period cannot exceed 70 years. Setting a value greater than 70 years results in an error.

Example 60

To set the min-retention-period to 24 months for mtree1: **`# mtree retention-lock set min-retention-period 24mo mtree /data/col1/mtree1`**

`mtree retention-lock show {min-retention-period | max-retention-period} mtree` *`mtree-path`*

Show the minimum or maximum retention period for the specified MTree. Role required: admin, user, backup-operator, security, none.

`mtree retention-lock status mtree` *`mtree-path`*

Show Retention Lock status for the specified MTree. Possible values are enabled, disabled, previously enabled, and MTree Retention Lock mode: Compliance or Governance. Role required: admin, user, backup-operator, security, none.

mtree show

`mtree show compression {`*`mtree-path`*` | tenant-unit` *`tenant-unit`*`} [tier {active | archive}] [summary | daily | daily-detailed] [last` *`n`* `{hours | days | weeks | months} | start` *`date`* `[end` *`date`*`]]`

Display compression statistics for a specific MTree. Values are reported in Gigibytes (GiB). Running the command without arguments generates default output that displays a summary of compression statistics for all files and directories in the file system for the last 7 days and the last 24 hours. Role required: admin, user, backup-operator, tenant-admin, tenant-user, security, none.

Argument Definitions

mtree-path
The pathname of the MTree for which to display compression statistics.

tenant-unit
The basic unit of a multi-tenancy configuration. A tenant unit is a secure, isolated partition for tenant-specific data and control flow within a Data Domain system.

tier {active | archive} (Optional)
Display results for the specified tier.

summary (Optional)
Display all compression statistics, summarized as:

- Data written in the last 7 days. By including the last *n* option or the start *date* option, you can display statistics for a time frame other than the last 7 days.
- Data written in the last 24 hours.

daily (Optional)
In addition to the summary output, display detailed information for each day, over the previous four full weeks, plus the current partial week. This option is not available if you specify a file or directory name.

daily-detailed (Optional)
Display the daily output and include the following information for each day. This option is not available if you specify a file or directory name.

last *n* {hours | days | weeks | months}(Optional)
In the summary portion of the output, display file system compression statistics for the specified time frame instead of for the past 7 days. The statistics for the last 24 hours remain in the summary output. If you specify a file or directory name, you cannot use this option with the weeks keyword or the months keyword.

start *date* (Optional)
In the summary portion of the output, display file system compression statistics for the time frame that begins on the specified day instead of the past 7 hours. The statistics for the last 24 hours remain in the summary output. If you specify a time frame less than the previous four weeks, plus the current full week, the daily or daily-detailed output (if specified) is truncated to the shorter time frame.

Specify *date* in the format *yyyy-mm-dd* (for example, 2013-04-07). By default, the last day of the time frame specified with this argument is the most recent, full day elapsed.

end *date* (Optional)
Valid only if the start option is used. In the summary portion of the output, display file system compression statistics for the time frame that ends on the specified day.

`mtree show performance {`*`mtree-path`*` | tenant-unit `*`tenant-unit`*`} [interval `*`n`*` {mins | hours}] [last `*`n`*` {hours | days | weeks | months} | start `*`MMDDhhmm[[CC]YY]`*` [end `*`MMDDhhmm[[CC]YY]`*`]]`
Displays MTree performance statistics. Replicate write data is not included in the output. Role required: admin, user, backup-operator, tenant-admin, tenant-user, security, none.

Argument Definitions

mtree-path
The pathname of the MTree for which to display performance statistics.

tenant-unit
The basic unit of a multi-tenancy configuration. A tenant unit is a secure, isolated partition for tenant-specific data and control flow within a Data Domain system.

interval *mins* or *hours* (Optional)
The interval is an optional number of minutes or hours.

last *n* {hours |days | weeks | months}
In the summary portion of the output, display file system performance statistics for the specified time frame instead of for the past 7 days. The statistics for the last 24 hours remain in the summary output. If you specify a file or directory name, you cannot use this option with the weeks keyword or the months keyword.

start (Optional)
In the summary portion of the output, display file system performance statistics for the time frame that begins on the specified day instead of the past 7 hours. The statistics for the last 24 hours remain in the summary output. If you specify a time frame less than the previous four weeks, plus the current full week, the daily or daily-detailed output (if specified) is truncated to the shorter time frame. Specify the starting date in the format: MMDDhhmm[[CC]YY]

end (Optional)
Valid only if the start option is used. In the summary portion of the output, display file system performance statistics for the time frame that ends on the specified day. Specify the ending date in the format: MMDDhhmm[[CC]YY]

Example 61

```
# sysadmin@ddr9# mtree show performance /data/col1/55_source
INTERVAL: 10 mins
"-" indicates that the data is not available for the intervals

Date         Time    Throughput          Streams
YYYY/MM/DD   HH:MM   read      write      rd/wr/r+/w+
                     MB/s      MB/s          #
-----------------    ----------------    -------------
2014/01/09 15:10     0.00    0.00        0/0/0/0
2014/01/09 15:20     0.00    41.66       0/3/0/0
2014/01/09 15:30     0.00    49.85       0/51/0/0
2014/01/09 15:40     0.00    23.04       0/51/0/0
```

mtree undelete

`mtree undelete` *mtree-path*
Mark as not deleted the marked-for-deletion MTree at the specified path. This command reverses a previous `mtree delete` command. Role required: admin.

Note

To undelete an MTree, cleaning must not have run before executing the `undelete` command.

Example 62

To reverse a previous `mtree delete` command request that included the MTree at `/data/col1/myMTree`:

```
# mtree undelete /data/col1/myMTree
```

CHAPTER 20

ndmpd

The `ndmpd` command is the top-level command for the NDMP (Network Data Management Protocol) daemon running on a Data Domain system. The NDMP daemon provides access to VTL-created devices using the NDMP version 4 protocol. Use of this command requires a VTL license.

This chapter contains the following topics:

ndmpd Change History

There have been no changes to this command since the 5.4 release.

ndmpd Guidelines and Restrictions

A VTL used by the NDMP (Network Data Management Protocol) tapeserver must be in the TapeServer access group.

ndmpd disable

`ndmpd disable`
Disable the NDMP (Network Data Management Protocol) daemon.

Role required: admin.

ndmpd enable

`ndmpd enable`
Enable the NDMP (Network Data Management Protocol) daemon.

Role required: admin.

ndmpd option

`ndmpd option reset` *`option-name`* `| all`
Reset all NDMP (Network Data Management Protocol) daemon options or just a specific option

Role required: admin.

`ndmpd option set` *`option-name value`*
Set a specific NDMP daemon option.

Role required: admin.

`ndmpd option show` *`option-name`* `| all`
Show the values for all NDMP daemon options or just for a specific option.

Role required: admin.

Argument Definitions

option-name
The specific NDMP (Network Data Management Protocol) daemon option, which can be authentication, debug, port, or preferred-ip.

value
The value for the specific option.

ndmpd show

`ndmpd option show` *`option-name value`*
View all NDMP (Network Data Management Protocol) daemon options or a specific option.

Role required: admin.

`ndmpd show devicenames`
View the device name, VTL virtual name, SCSI vendor and product code, and the serial numbers of devices controlled by the NDMP daemon. Typically, this information is displayed during device discovery and configuration. However, you can use this command to verify the VTL TapeServer group configuration and perform a manual configuration, if required.

If there is no output in the NDMP Device column, either the VTL service is not running or there are no devices registered with the VTL TapeServer. A series of hyphens in the NDMP Device column means the VTL service is running on the system, but has not registered the devices. Restart the VTL service to correct this behavior. If this problem persists, go to EMC Online Support for assistance.

Role required: admin.

`ndmpd show sessions`
View active sessions.

Role required: admin.

`ndmpd show stats` *`session-id`* | `all`
View statistics of a single session or all sessions. Session numbers are displayed by `ndmpd show sessions`.

Role required: admin.

ndmpd status

`ndmpd status`
Display the NDMP (Network Data Management Protocol) daemon status.

Role required: admin.

ndmpd stop

`ndmpd stop session` *`session-id`* | `all`
Stop all NDMP (Network Data Management Protocol) sessions or stop a single session.

Role required: admin.

ndmpd user

`ndmpd user add` *`user-name`*
Add (only) one user name for the NDMP (Network Data Management Protocol) daemon md5 authentication.

Role required: admin.

`ndmpd user del` *`user-name`*
Delete the configured NDMP daemon user.

Role required: admin.

`ndmpd user modify` *`user-name`*
Modify the name of the NDMP daemon md5 user.

Role required: admin.

`ndmpd user show`

View the NDMP daemon user.

Role required: admin.

CHAPTER 21

net

The `net` command manages the use of virtual interfaces, DHCP, DNS, and IP addresses, and displays network information and status.

Federal certification requirements state that the DD OS must be IPv6-capable and that interoperability with IPv4 be maintained in an heterogeneous environment. As a result, several net command options include arguments for both versions of Internet Protocol. Collection, directory, and MTree replication are supported over IPv6 networks, which allows you to take advantage of the IPv6 address space. Simultaneous replication over IPv6 and IPv4 networks is also supported, as is Managed File Replication using DD Boost. IPv6 addresses are not supported for CIFS.

If you do not specify an IP version, the default is IPv4 to maintain compatibility with DD OS versions prior to 5.2. The exception is `show` commands. If the version is not specified in the `show` command option (as in `route show table`), both address versions are displayed. To view the IPv4 routes only, you must specify the `IPv4` argument.

For some commands, you must include the IPv6 command argument if the host is to be accessed using its IPv6 address. This is required when a hostname is specified and the host name format resembles an IPv4 address.

This chapter contains the following topics:

net Change History

This section provides a list of changes since the 5.4 release, for all 5.5.x releases, in order of most recent release to first release.

New Commands in DD OS 5.5.1

net ddns reset TSIG-key
Clear the TSIG key (DDNS server user name) and secret (password).

net ddns set TSIG-key *key* TSIG-secret *secret*
Set the TSIG key and secret.

Modified Arguments in DD OS 5.5.1

net config *ifname* {*ipaddr* netmask *mask* | dhcp {yes | no} | [*ipv6addr*]} {[autoneg] | [duplex {full | half} speed {10|100|1000|10000}] [up | down] [mtu {*size* | default}] [txqueuelen *size*]
Added the option to select either IPv4 or IPv6 for DHCP communication.
`net config ifname {ipaddr netmask mask | [ipv6addr | [dhcp {yes [ipversion {ipv4 | ipv6}] | no}]} {[autoneg] | [duplex {full | half} speed {10|100|1000|10000}] [up | down] [mtu {size | default}] [txqueuelen size]`

net create interface {*physical-ifname* | *virtualifname*} {vlan *vlan-id* |alias *alias-id*}
The alias option is deprecated. To create an alias, use net config. The new syntax is
`net create interface {physical-ifname | virtualifname} {vlan vlan-id}`

net ddns add {*ifname-list* | all }
There is no change for this command when DDNS is enabled for Windows environments. When DDNS is enabled for UNIX environments, this command adds an interface to DDNS and specifies the hostname assigned to the interface. The new syntax is
`net ddns add {ifname-list | all | ifname interface-hostname {auto | host | hostname}}`

net ddns enable
This command now allows you to enable DDNS for either the Windows or the UNIX environment. The new syntax is
`net ddns enable [windows | unix [TSIG-key key TSIG-secret secret]]`

Modified Output in DD OS 5.5.1

net ddns register
A new error message provides information on DNS server access errors when operating in UNIX mode.

net ddns show
When operating in UNIX mode, this command now indicates the UNIX mode.

net ddns status
This command now indicates whether DDNS is enabled for Windows mode or UNIX mode.

Modified Behavior in DD OS 5.5.1

net ddns reset

When operating in UNIX mode, this command deletes the TSIG key and the interface selections.

New Commands in DD OS 5.5

net create interface {*physical-ifname* | *virtualifname*} {vlan *vlan-id* |alias *alias-id*}

The alias option is deprecated. To create an alias, use net config. The new syntax is `net create interface {physical-ifname | virtualifname} {vlan vlan-id}`

net modify *virtual-ifname* bonding {aggregate | failover}

Change the behavior of the specified virtual interface from aggregate to failover for from failover to aggregate.

Modified Arguments in DD OS 5.5

net aggregate del *virtual-ifname* interfaces *physical-ifname-list*

Added the option to specify all interfaces.
`net aggregate del virtual-ifname interfaces {physical-ifname-list | all}`

net config *ifname* {[[*ipaddr*] [netmask *mask*] [dhcp {yes | no}]] | [*ipv6addr*]} {[autoneg] | [duplex {full | half} speed {10 | 100 | 1000 | 10000}] [up | down] [mtu {*size* | default}]

Added the option to set the transmit queue length.
`net config ifname {ipaddr netmask mask | dhcp {yes | no} | [ipv6addr]} {[autoneg] | [duplex {full | half} speed {10|100|1000|10000}] [up | down] [mtu {size | default}] [txqueuelen size]`

net failover del *virtual-ifname* interfaces *physical-ifname-list*

Added the option to specify all interfaces.
`net failover del virtual-ifname interfaces {physical-ifname-list | all}`

Modified Output in DD OS 5.5

net show settings

Displays any IPv6 addresses associated with each port.

Deprecated Commands in DD OS 5.5

net aggregate reset *virtual-ifname*

Use `net aggregate del` to delete physical interfaces from an aggregate virtual interface.

net failover reset *virtual-ifname*

Use `net failover del` to delete physical interfaces from a failover virtual interface.

net Guidelines and Restrictions

- Changes made by the net command to disabled Ethernet interfaces flush the routing table. EMC Data Domain recommends making interface changes only during

scheduled downtime. After making changes to disabled interfaces, you must reconfigure all routing rules and gateways.

- IPv4 is the default IP version.

net aggregate

`net aggregate add` *`virtual-ifname`* `interfaces` *`physical-ifname-list`* `[mode {roundrobin | balanced hash {xor-L2 | xor-L3L4| xor-L2L3} | lacp hash {xor-L2 | xor-L3L4 | xor-L2L3} [rate {fast | slow}] [up {`*`time`*` | default}] [down {`*`time`*` | default}]`

Add slave interfaces to an aggregate interface. Setting the mode is required on initial configuration and when there is no default aggregate mode, but optional when adding interfaces to an existing aggregate interface. Choose the mode compatible with the specifications of the system to which the ports are attached. Balanced and lacp modes require a hash. Role required: admin.

Example 63

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
```

Argument Definitions

round robin
Packets are transmitted sequentially, beginning with the first available link and ending with the last link in the aggregated group.

balanced
Data is sent over interfaces as determined by the hash method selected. This requires the associated interfaces on the switch to be grouped into an Ethernet trunk. Requires a hash.

lacp
LACP is a link aggregation mode based on the Link Aggregation Control Protocol (IEEE 802.3ad). From a switch perspective this configuration is always an active LACP configuration. It cannot be set to passive. LACP communicates with the other end to coordinate which links within the bond are available. When the this mode is selected, both ends must be configured with LACP. Requires a hash.

An interface must not only have carrier up, but also must be able to communicate with its directly attached partner. This provides a better port fail recovery than failover bonding; however, the LACP port must reside on a single switch except for special cases of virtual switch ports. Therefore to fail across switches, failover bonding must be used.

rate

Specifies how often an LACP message is sent to the switch or system that is connected to the Data Domain system. The message identifies the aggregated interface. This acts as a type of heartbeat. Slow sends the message once every 30 seconds. It is the default. Fast sends the message every second.

The rate determines how fast the lacp will recognize when an interface cannot be used and when it can. If 30 seconds is too long it can be set to fast (1 second), but fast means there is more traffic comprised of small packets (about the size of a TCP ACK packet) across all aggregated lacp interfaces. With 10 Gb speed consider the potential for losing connections with a rate of 30 seconds.

xor-L2

Transmission of packets from a specific slave interface is based on static balanced mode or LACP mode aggregation with an XOR based on a hash policy. An XOR of source and destination MAC addresses is used to generate the hash.

xor-L2L3

Transmission of packets from a specific slave interface is based on static balanced and LACP mode aggregation with an XOR based on a hash policy. An XOR of source and destination's upper layers (L2 and L3) protocol information is used to generate the hash.

xor-L3L4

Transmission of packets from a specific slave interface is based on static balanced and LACP mode aggregation with an XOR based on a hash policy. An XOR of source and destination's upper layers (L3 and L4) protocol information is used to generate the hash.

up, down

The length of delay allowed before the link is considered up or down. A down interface must be up for interval configured in *time* to be considered up. Conversely, an up interface must be down for the interval configured in *time* to be considered down and not available.

If a link is up, the interface carrier must be missing for the amount of time specified by the down argument before the link is designated down. Default for up/down times is 29.7 seconds. Up/down times are rounded down to a multiple of 0.9 seconds. For example if 10 seconds is configured, 9.9 seconds is used.

When the link is down:

- Data is no longer sent to the interface.
- For an aggregation bonding, aggregation is recalculated.
- For a failover bonding, if the affected interface is the active interface, then the active interface is switched to another interface that is up.

The interface carrier must be present for the amount of time specified by the up argument before the link is designated up.

When the link is up:

- Data can be sent over it.
- For an aggregation bonding, the aggregation is recalculated to include the up link.

For a failover bonding, nothing more is done; however, if the up interface is the primary or sole, up slave interface, then it is also marked as the active interface.

`net aggregate del` *virtual-ifname* `interfaces {`*physical-ifname-list* `| all}`
Delete slave interfaces from the list of the aggregate virtual interface. Role required: admin.

Example 64

To delete physical interfaces eth2a and eth3a from the aggregate virtual interface veth1:

```
# net aggregate del veth1 interfaces eth2a,eth3a
```

`net aggregate modify` *virtual-ifname* `[mode {roundrobin | balanced hash {xor-L2 | xor-L3L4| xor-L2L3} | lacp hash {xor-L2| xor-L3L4 | xor-L2L3} [rate {fast | slow}]}] [up {`*time* `| default}] [down {`*time* `| default}]`
Change the configuration of an aggregate interface. You must indicate the mode the first time. Choose the mode compatible with the specifications of the system to which the ports are attached. Balanced and lacp modes require a hash. Role required: admin.

Example 65

Use the following command to change link aggregation on virtual interface veth1 to mode lacp hash xor-L2. Stating the previous condition is not required. The listed conditions replace the previous settings except on the current slave interfaces, which remain slaves to the virtual interface. Slaves may be added by this command, but none are removed.

```
# net aggregate modify veth1 mode lacp hash xor-L2
```

`net aggregate show`
Display basic information on the aggregate setup. If the bonded interface has not been brought up, output displays `No interface in the aggregate mode`. Role required: admin, security, user, backup-operator, or none.

Note

With the exception of `net aggregate show`, `net aggregate` commands control link aggregation, which provides improved network performance and resilience by using two or more network ports in parallel. Note that link aggregation and Ethernet trunking are synonymous. The recommended and supported maximum is four ports, but there are no restrictions on the Data Domain system for having more aggregate slaves.

net config

`net config` *ifname* `{[`*ipaddr* `[netmask` *mask*`]] | [`*ipv6addr/prefix*`] | [dhcp {yes [ipversion {ipv4 | ipv6}] | no}]} {[autoneg] | [duplex {full | half} speed {10|100|1000|10000}] [up | down] [mtu {`*size* `| default}] [txqueuelen` *size*`]`
Display the physical interface configuration or configure a base interface or an alias interface. A base interface is a physical, virtual, or VLAN interface to which you can add one IP address either manually or through DHCP. An alias interface is used to add an additional IP address to a base interface, and you can create multiple alias interfaces to add multiple IP addresses to a base interface.

Note

An alias interface does not operate as an independent interface. DD OS generates statistics and supports additional configuration settings only for a base interface. The only function of an alias interface is to add an additional IP address to the base interface.

To create an alias interface, enter the base interface and alias name in the following format: *base_interface*:*alias_name* and specify an IPv4 or IPv6 address. The following are some sample alias names.

- eth5a:35—The base interface is physical interface eth5a, and the alias name is 35.
- veth4:26—The base interface is virtual interface veth4, and the alias name is 26.
- eth5a.82:162—The base interface is VLAN interface eth5a.82, and the alias name is 162.

To delete an alias interface, assign the 0 value to the IP address as follows: **`net config eth0a:200 0`**

Role required: admin.

Argument Definitions

autoneg
Specify this option to configure the interface to autonegotiate the duplex and speed settings with the remote interface.

dhcp {yes [ipversion {ipv4 | ipv6}] | no}
Set the `dhcp` option to yes to configure the interface to receive the IP address configuration from a DHCP server, and set this option to no when you want to manually configure the IP address. The default option requests an IPv4 address from DHCP, but you can select either IPv4 or IPv6 when you enable DHCP. When you use DHCP, the IP address delivered by DHCP replaces any static IP address previously configured for the base interface.

Note

If you choose to obtain the network settings through DHCP over IPv6, you must manually configure the hostname with the `net set hostname` command or with DD System Manager at **Hardware** › **Network** › **Settings**.

duplex {full | half} speed {10|100|1000|10000}
Specify this option when you want to manually configure the duplex setting or speed. The speed settings are 10, 100, 1,000, or 10,000 Mbps. This option automatically disables autonegotiation on the interface.

ifname
Specify the interface to configure. To display the available physical interfaces, enter `net show hardware`. The interface names appear in the Port column. To create an alias interface, enter the alias in the following format: *base_interface*:*alias_name*. The alias name must be a number in the range of 1 to 9999.

ipaddr [netmask *mask*]
Specify an IPv4 address for the interface. The `dhcp` option must be set to no to support manual IP address configuration.

Use the `netmask` option to specify a network mask that is different from the default netmask. The `netmask` can only be specified when an IPv4 address is specified.

ipv6addr/prefix
Specify an IPv6 address for the interface. The `dhcp` option must be set to no to support manual IP address configuration.

If an IPv6 address is specified, there is no associated netmask. Instead, a prefix length is used to determine the subnet. The default prefix length is 64. To use a prefix length different from 64, it must be specified with the address by adding a forward slash followed by a number. For example, if the prefix length is 52, the notation is: 2026:3456:cafe::f00d:1/52.

Note

DD140, DD160, DD610, DD620, and DD630 systems do not support IPv6 on interface eth0a (eth0 on systems that use legacy port names) or on any VLANs created on that interface.

mtu {*size* | default}
The range for the MTU size is 350 - 9000 for IPv4 and 1280 - 9000 for IPv6. To ensure backward compatibility DD OS accepts an MTU size of 9014, but sets it to 9000 if the MTU requested is greater than 9000 and less than or equal to 9014.

txqueuelen *size*
Specify the transmit queue length. The range is 500 to 10,000 packet pointers, and the default value is 1000.

up | down
Use the `up` argument to bring up an interface without an IP address. (Using `net enable` fails if no IP address is given.) Use the `down` argument to bring down an interface.

Note

If no address is given, the `up` option might fail because there is no registry entry for an IP address. This typically occurs after a fresh install. If this occurs, specify an address of 0 to allow a registry address location to be created.

Example 66

The following example shows an excerpt from the `net config` display when no arguments are entered.

```
eth1d     Link encap:Ethernet  HWaddr 00:1B:21:5F:E2:4D
          inet6 addr: 2100:bad:dead:f00d::e4b:100/64 Scope:Global
          inet6 addr: 2100:dead:f00d:cafe::deed:3e1d/64 Scope:Global
          inet6 addr: 2100:bad:dead:f00d::e4b:210/64 Scope:Global
          inet6 addr: fe80::21b:21ff:fe5f:e24d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:37274 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:2431901 (2.3 MiB)

eth1d:10  Link encap:Ethernet  HWaddr 00:1B:21:5F:E2:4D
          inet addr:192.168.141.20  Bcast:192.168.141.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

eth1d:100  IPv6 alias address, 2100:bad:dead:f00d::e4b:100/64, is on the interface eth1d
when up

eth1d:200 Link encap:Ethernet  HWaddr 00:1B:21:5F:E2:4D
```

Example 66 (continued)

```
          inet addr:192.168.141.200  Bcast:192.168.141.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

eth1d:210  IPv6 alias address, 2100:bad:dead:f00d::e4b:210/64, is on the interface eth1d
when up
```

Interface eth1d represents the physical interface. Interfaces eth1d:10 and eth1d:200 are alias interfaces that each add an IPv4 address to the base interface, and eth1d:100 and eth1d:210 are alias interfaces that add IPv6 addresses to the same base interface. The IPv6 alias addresses are available when the base interface is in the running state and the alias interface state is *up.* Notice that the IPv6 alias addresses in the example above are displayed with the alias interfaces and the base interface.

Example 67

The following example adds an alias named 200 to the eth0a interface and assigns an IPv6 address to it.

```
# net config eth0a:200 2620:0:170:1a04:28c:faff:fe05:6c91/64
Creating interface ...
Done.
Configuring interface...
done.
```

Example 68

The following example deletes alias 200 from the eth0a interface.

```
# net config eth0a:200 0
Alias is destroyed.
```

`net config` *`ifname`* `type {none | management | replication | cluster}`

Configure a label for the intended traffic type on the interface. The system does not use the label to enforce the specified traffic type; this is only a label. Role required: admin.

Argument Definitions

cluster
This was previously used for GDA environments and does not apply to any traffic types in this release.

management
Indicates that the interface is to support system management traffic.

none
Indicates that no traffic type label is specified for this interface.

replication
Indicates that the interface is to support replication traffic.

net congestion-check

`net congestion-check modify [sample-interval` *`secs`*`] [capture-window` *`secs`*`] [every` *`mins`*`] [detailed {on | off}] [logfile` *`filename`*`] [logfilev6` *`filename`*`] [iperf-client {none | iperf-`

server-host | *iperf-server-ipaddr*} [nodelay {on | off}] [port {*port* | default}] [window-size *bytes*] [connections *count*] [data {random|default}]}]

Congestion data is collected during a period of time defined by the *capture window* argument. Within the capture window, data is captured at intervals defined by the `sample-interval` argument. If the `every` argument is non-zero, a new capture window starts at intervals determined by the `every` argument. For example, if the capture window is 60 seconds, the sample interval is 5 seconds, and the every argument is set to 60, data is collected every 60 minutes for a period of 60 seconds at 5 second intervals. The output concludes displays as one line per remote IP address.

This command modifies options for the congestion monitor whether or not the monitor program is activated. (The congestion monitor is activated by the net congestion-check start command.) The settings configured with this command are stored in the registry and replace the default values used by `net congestion-check start` command. If the congestion monitor is scheduled, the new registry values are used when it runs. If the monitor is not scheduled, the values are used as defaults when it is started. Typically this command option is used after the monitor is scheduled to run and the user does not want to stop and restart the monitor.

Output values for rates and error numbers are added together. Values that may increase or decrease, such as the capture-window, are averaged over time. Role required: admin.

Argument Definitions

capture-window

Specify the period during which data is captured. The initial value is 60 seconds. The configured value must be less than the `every` argument and greater than the `sample-interval`argument.

detailed

By default, only basic information is saved, but setting the argument to `on` causes more data to be saved. The basic setting is mainly for replication on the source system and focuses on congestion conditions between the source and destination. The detailed `on` argument adds receive information and other entries useful for the general network environments of the Data Domain system. The initial value is `off`.

every

Specify the period between the start of each capture window. The initial period is 60 minutes. If set to zero the capture window is run once only. The configured period must be greater than that for the `capture-window` argument.

iperf-client

This command option determines whether or not the iperf client can perform throughput tests during a network congestion check. The `none` argument prevents the iperf client from running during a network congestion check. If iperf was previously enabled and is no longer needed, use the `none` argument to disable iperf use by the congestion monitor. The initial value is `none`.

The `iperf-server-host` and `iperf-server-ipaddr` arguments enable the iperf client to run during congestion checks and specify a target iperf server hostname or IP address. To enable iperf throughput testing, you must configure iperf to communicate with a remote system using the appropriate server name or IP address and the appropriate port number.

If the congestion monitor requires iperf data and if iperf is enabled, the iperf test is started at the beginning of a capture window. Iperf is disruptive to the network and should not be left on for a long time, especially if there is other traffic using the network. If you want to control iperf operation manually, you can start iperf with the `net iperf` command before the congestion check is performed. The advantage of letting the congestion-check manage iperf operation is that iperf is run only when the congestion-check requires it. Otherwise iperf does not run.

Options for modifying or starting iperf during the capture window are as follows.

connections

The number of connections to use. Must be greater than zero. Default is 1, which is typically satisfactory if the window size is set appropriately.

data

An in-memory random data generator. This would be used if a WAN accelerator was in the path thereby preventing the generator from providing elevated bandwidth numbers.

nodelay

On means do not wait for ACK. Off means wait for each buffer to be sent before sending the next.

port

The port number to use with iperf. Default is 5002, which is one more than the iperf default 5001.

window-size

The size of the socket buffer to use. Default is 32000. For long latencies, this size may be too small. Consider setting the size to 250000 or 10000000.

logfile

Set the log file name used to save the data collected. The initial default is `/ddvar/log/default/congestion.log`.

The file name should not be changed unless absolutely required. The main concern is the default file name is on a rotation system where the file size cannot exceed 10 MB and up to 10 files only are saved for a maximum of 100 MB of disk space. Changing the file name voids the space restrictions, meaning there is no limit to the space that may be taken.

sample-interval

Specify the sample period within the capture window. The initial value is 4 seconds. The value of the `sample-interval` argument must be less than the value of the `capture-window` argument.

`net congestion-check run [sample-interval` *`secs`*`] [capture-window` *`secs`*`] [every` *`mins`*`] [detailed {on | off}] [logfile` *`filename`*`]`

`[{iperf-client {none | {`*`iperf-server-host`*` | `*`iperf-server-ipaddr`*`} [nodelay {on | off}] [port {`*`port`*` | default}] [window-size `*`bytes`*`] [connections `*`count`*`] [data {random|default}]}]`
Run the congestion check program and display the results as screen output when the `capture-window` time is complete. When the command option is entered without arguments, defaults are used. When the command option includes arguments, the arguments override the defaults during the procedure but return to the configured defaults after the procedure concludes. Default values for the `run` command are always the same and are not affected by the `net congestion-check modify` or the `net congestion-check start` commands.

Argument Definitions

capture-window

Specify the period during which data is captured. The default value is 60 seconds. The configured value must be less than the `every` argument and greater than the `sample-interval`argument.

detailed

By default, only basic information is saved, but setting the argument to `on` causes more data to be saved. The basic setting is mainly for replication on the source system and focuses on congestion conditions between the source and destination. The detailed `on` argument adds receive information and other entries useful for the general network environments of the Data Domain system. The default is `off`.

every

Specify the period between the start of each capture window. The default value is 0, which specifies to run the capture window only once. If you specify a non-zero value, the configured period must be greater than that for the `capture-window` argument.

iperf-client

This command option determines whether or not the iperf client can perform throughput tests during a network congestion check. The `none` argument prevents the iperf client from running during a network congestion check. If iperf was previously enabled and is no longer needed, use the `none` argument to disable iperf use by the congestion monitor. The default value is `none`.

The `iperf-server-host` and `iperf-server-ipaddr` arguments enable the iperf client to run during congestion checks and specify a target iperf server hostname or IP address. To enable iperf throughput testing, you must configure iperf to communicate with a remote system using the appropriate server name or IP address and the appropriate port number.

If the congestion monitor requires iperf data and if iperf is enabled, the iperf test is started at the beginning of a capture window. Iperf is disruptive to the network and should not be left on for a long time, especially if there is other traffic using the network. If you want to control iperf operation manually, you can start iperf with the `net iperf` command before the congestion check is performed. The advantage of letting the congestion-check manage iperf operation is that iperf is run only when the congestion-check requires it. Otherwise iperf does not run.

Options for modifying or starting iperf during the capture window are as follows.

connections

The number of connections to use. Must be greater than zero. Default is 1, which is typically satisfactory if the window size is set appropriately.

data

An in-memory random data generator. This would be used if a WAN accelerator was in the path thereby preventing the generator from providing elevated bandwidth numbers.

nodelay

On means do not wait for ACK. Off means wait for each buffer to be sent before sending the next. The default is off.

port

The port number to use with iperf. Default is 5002, which is one more than the iperf default 5001.

window-size

The size of the socket buffer to use. Default is 32000. For long latencies, this size may be too small. Consider setting the size to 250000 or 10000000.

logfile

Set the log file name used to save the data collected. The initial default is `/ddvar/log/default/congestion.log`.

The file name should not be changed unless absolutely required. The main concern is the default file name is on a rotation system where the file size cannot exceed 10 MB and up to 10 files only are saved for a maximum of 100 MB of disk space. Changing the file name voids the space restrictions, meaning there is no limit to the space that may be taken.

sample-interval

Specify the sample period within the capture window. The default value is 4 seconds. The value of the `sample-interval` argument must be less than the value of the `capture-window` argument.

```
net congestion-check start [sample-interval secs] [capture-
window secs] [every mins] [detailed {on | off}] [logfile
```

filename] [{iperf-client {none | {*iperf-server-host* | *iperf-server-ipaddr*} [nodelay {on | off}] [port {*port* | default}] [window-size *bytes*] [connections *count*] [data {random| default}]}]

Start the congestion monitor and schedule when it is to be run using the time arguments: `sample-interval`, `capture-window`, and `every`. When the command option is run with arguments, the arguments override the defaults and become the default by being placed in the registry. The remaining arguments of `net congestion-check start` command are used to configure in detail how the monitor is run.

Note

After entering the command, there is a slight delay during which the process (`netmon`) actually starts the monitor. After the monitor is started the specified time arguments take over. To get information immediately, use the `net congestion-check run` command instead.

Output is one line per external destination. All connections to and from an external address are merged into a single line of data.

Value types from the output vary. Amounts of data or packets increase. These amounts are added together across all connections to a specific IP address to give the total value to or from the external location. Rates are relatively constant but are also added together to give the total flow rate to the pipe at the remote location. Other values are relatively static across all connections, such as the mss, rtt, window scale factor, or congestion window. These are given as an average with the minimum and maximum. Errors and loses are treated the same as rates and are added across all interfaces. Role required: admin.

Argument Definitions

capture-window

Specify the period during which data is captured. The initial value is 60 seconds. The configured value must be less than the `every` argument and greater than the `sample-interval`argument.

detailed

By default, only basic information is saved, but setting the argument to `on` causes more data to be saved. The basic setting is mainly for replication on the source system and focuses on congestion conditions between the source and destination. The detailed `on` argument adds receive information and other entries useful for the general network environments of the Data Domain system. The initial value is `off`.

every

Specify the period between the start of each capture window. The initial period is 60 minutes. The configured period must be greater than that for the `capture-window` argument. Because this command configures an ongoing monitor, value 0 is not supported.

iperf-client

This command option determines whether or not the iperf client can perform throughput tests during a network congestion check. The `none` argument prevents the iperf client from running during a network congestion check. If iperf was previously enabled and is no longer needed, use the `none` argument to disable iperf use by the congestion monitor. The initial value is `none`.

The `iperf-server-host` and `iperf-server-ipaddr` arguments enable the iperf client to run during congestion checks and specify a target iperf server hostname or IP address. To enable iperf throughput testing, you must configure iperf to communicate with a remote system using the appropriate server name or IP address and the appropriate port number.

If the congestion monitor requires iperf data and if iperf is enabled, the iperf test is started at the beginning of a capture window. Iperf is disruptive to the network and should not be left on for a long time, especially if there is other traffic using the network. If you want to control iperf operation manually, you can start iperf with the `net iperf` command before the congestion check is performed. The advantage of letting the congestion-check manage iperf operation is that iperf is run only when the congestion-check requires it. Otherwise iperf does not run.

Options for modifying or starting iperf during the capture window are as follows.

connections

The number of connections to use. Must be greater than zero. Default is 1, which is typically satisfactory if the window size is set appropriately.

data

An in-memory random data generator. This would be used if a WAN accelerator was in the path thereby preventing the generator from providing elevated bandwidth numbers.

nodelay

On means do not wait for ACK. Off means wait for each buffer to be sent before sending the next.

port

The port number to use with iperf. Default is 5002, which is one more than the iperf default 5001.

window-size

The size of the socket buffer to use. Default is 32000. For long latencies, this size may be too small. Consider setting the size to 250000 or 10000000.

sample-interval

Specify the sample period within the capture window. The initial value is 4 seconds. The value of the `sample-interval` argument must be less than the value of the `capture-window` argument.

`net congestion-check status`

Display the state of the congestion monitor. The congestion monitor is started when the `net congestion-check start` command is issued. The `status` argument displays the configured timings, the level of logging, the log file, the monitored connections, if the monitor is actually running or scheduled to run, and if iperf is specified to run. It also shows if iperf is currently running and which connections are being monitored. Role required: admin, security, user, backup-operator, or none.

`net congestion-check stop`

The congestion monitor is run when the `net congestion-check start` command is issued. A message notifies the user if the configuration monitor is not scheduled and

no action is taken. If the congestion monitor is scheduled, this command option unschedules the procedure. If the congestion monitor is running, this command option stops the procedure and unschedules it. Role required: admin.

net create

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

Create a VLAN interface on the specified physical or virtual interface. The VLAN is created immediately in the kernel, and the number given must be between 1 and 4094 inclusive. There must be a matching VLAN number on the switch or other systems to transfer packets to the interface. Role required: admin.

`net create virtual veth`*`id`*

Create a virtual interface. The virtual interface name veth-*id* must begin with veth. The remainder of the name is a decimal number. Interface names must be unique.

There are no restrictions except for the size and the number. The maximum size for an interface name is 15 characters, which includes VLAN, alias names, and the associated dot and colon. The virtual interface name must be kept at a minimum. The maximum is 9999, but EMC recommends using a number in the range of 0 to 99.

The number of virtual interfaces cannot exceed the number of physical interfaces. For example, if there are 10 physical interfaces there can be no more than 10 virtual interfaces. Role required: admin.

net ddns

`net ddns add {`*`ifname-list`* `| all |` *`ifname`* `interface-hostname {auto | host |` *`hostname`*`}}`

Add interfaces to the Dynamic DNS (DDNS) registration list. Role required: admin.

Note

When DDNS is configured for UNIX mode, this feature supports physical interfaces and aliases for physical interfaces. In this release, VLAN and virtual interfaces (and any aliases for those interfaces) are not supported in DDNS UNIX mode.

Argument Definitions

all
When DDNS is enabled for the Windows environment, this option specifies that host names be registered for all interfaces.

ifname
When DDNS is enabled for the UNIX environment, this option specifies an interface to be registered with DDNS.

ifname-list
When DDNS is enabled for the Windows environment, this option specifies that host names be registered for the specified interfaces.

interface-hostname
When DDNS is enabled for the UNIX environment, this argument defines the hostname that is registered with DDNS.

auto
This argument selects the hostname format *hostname-ifname*. If the hostname is Corporate and the interface name is eth0a, the hostname for the interface is Corporate-eth0a.

host
This argument selects the system hostname as the interface hostname. If the system hostname is Corporate and the interface name is eth0a, the hostname for the interface is Corporate.

hostname
This argument specifies a hostname to assign to the interface. If the specified hostname is America and the interface name is eth0a, the hostname for the interface is America.

`net ddns del {`*`ifname-list`*` | all}`
Remove one or all interfaces from the DDNS registration list. Role required: admin.

`net ddns disable`
Disable DDNS updates. Role required: admin.

`net ddns enable [windows | unix [TSIG-key `*`key`*` TSIG-secret `*`secret`*`]]`
Enable DDNS updates for either Windows or UNIX environments. Role required: admin.

Note

If DDNS is already enabled, you must disable DDNS before selecting a different mode.

Argument Definitions

TSIG-key
Specifies a DDNS user name for the UNIX environment.

TSIG-secret
Specifies a DDNS password for the UNIX environment.

`net ddns register`
Register configured interfaces with DNS. Role required: admin.

`net ddns reset`
Clear the DDNS interface list and disable registration. In Windows mode, the registration list is set to auto. In UNIX mode, the TSIG key is also deleted. Role required: admin.

`net ddns show`
In Windows mode, display the enabled interfaces. In UNIX mode, display the UNIX mode status and the enabled interfaces. Role required: admin, security, user, backup-operator, or none.

`net ddns status`
Display only the DDNS status, which can be enabled in Windows mode, enabled in UNIX mode, or disabled. Role required: admin, security, user, backup-operator, or none.

`net ddns reset TSIG-key`
Clear the TSIG key (DDNS server user name) and secret (password). Role required: admin.

`net ddns set TSIG-key `*`key`*` TSIG-secret `*`secret`*
Set the TSIG key and secret. Role required: admin.

net destroy

`net destroy {virtual-ifname | vlan-ifname | ipalias-ifname}`
Remove a VLAN, IP alias, or virtual interface. If a virtual interface has associated VLANs and aliases, or if a VLAN has associated aliases, the associated interfaces are also destroyed when the virtual interface or VLAN interface is destroyed. Role required: admin.

Example 69

To remove a VLAN named eth1a.35 and a virtual interface named veth23:2:

```
# net destroy eth1a.35
```

```
# net destroy veth23
```

net disable

`net disable ifname`
Disable an Ethernet interface on the Data Domain system and bring down the interface in the kernel. Role required: admin.

net enable

`net enable ifname`
Enable or reenable an Ethernet interface on the Data Domain system, where *ifname* is the name of an interface. This includes bringing up the interface to the RUNNING state and requires the interface to have an IP address. The address may already be saved in the registry or may come from DHCP. If the interface does not go into the RUNNING state, the command will fail and the interface is set to the DOWN state and set to disabled. Role required: admin.

net failover

`net failover add virtual-ifname interfaces ifname-list [primary ifname] [up {time | default}] [down {time | default}]`
Add network interfaces as slaves to a failover interface. The virtual interface must be created before you can use this command to add failover slaves. (Use `net show settings` to view all interfaces.) Allow one failover slave to be set as the primary and allow the up and down delays to be set. The slave interfaces must be in a down (disabled) state when added to the virtual interface. Note that the network interfaces can be aggregated interface. Role required: admin.

Example 70

The following command example associates a failover virtual interface named veth1 with the physical interfaces eth2a and eth3a and designates eth2a as the primary interface.

```
# net failover add veth1 interfaces eth2a eth3a primary eth2a
```

`net failover del` *virtual-ifname* `interfaces {`*physical-ifname-list* `| all}`
Delete slave interfaces from a failover interface. The freed interface remains disabled after being removed from the physical interface. Use commas, spaces, or both to separate list entries, or specify all to delete all slave interfaces. To delete a primary interface, use `net failover modify` to specify another interface as primary or set the primary to none. Role required: admin.

Example 71

To remove eth2a from the virtual interface veth1, which has eth2a and eth3a as slaves and eth3a as the primary interface:

```
# net failover del veth1 interfaces eth2a
```

`net failover modify` *virtual-ifname* `[primary {`*ifname* `| none}] [up {`*time* `| default}] [down {`*time* `| default}]`
Modify the primary network interface, the up /down times for a failover interface, or both. A down interface must be up for the amount of *time* to be designated up. An up interface must be down for the amount of *time* to be designated down.

The up and down time is given in milliseconds and is adjusted internally to the largest multiple of 900, less than or equal to the specified value. For example, if the time you want is 10 seconds and 10000 is specified, the actual value would be 9900. The default value is 30 seconds but the actual resulting value is 29.7 seconds.

A primary interface cannot be removed from failover. To remove a primary use `primary` *physical-ifname* `none` first. Role required: admin.

Example 72

```
# net failover modify veth1 up 5000 down 10000
```

The up time value used would be 4500 (4.5 seconds) and the down time value would be 9900 (9.9 seconds).

`net failover show`
Display all failover interfaces. This command shows what is configured at the bonding driver. To see what is in the registry, use the `net show settings` command.

The registry settings may be different from the bonding configuration. After creation, when interfaces are added to the virtual interface, the information is not sent to the bonding module until the virtual interface is brought up. Until that time the registry and the bonding driver configuration differ. Role required: admin, security, user, backup-operator, or none.

net hosts

`net hosts add {`*ipaddr* `|` *ipv6addr*`}` *host-list*
Add a host list entry. Associate an IP address with a hostname. The address can be a IPv4 or an IPv6. The hostname is a fully qualified domain name, a hostname, or an alias. The entry is added to the `/etc/hosts` file. Entries in the list can be separated by commas, spaces, or both. Role required: admin.

Example 73

To associate the fully qualified domain name bkup20.yourcompany.com and the hostname of bkup20 with an IP address of 192.168.3.3, enter the following command.

```
# net hosts add 192.168.3.3 bkup20.yourcompany.com bkup20
```

`net hosts del {`*`ipaddr`* `|` *`ipv6addr`*`}`
Delete a host list entry from the //`etc/hosts` file. Role required: admin.

`net hosts reset`
Clear the hosts list from the `/etc/hosts` file. Role required: admin.

`net hosts show`
Display hostnames and IP addresses from the `/etc/hosts` file. Role required: admin, security, user, backup-operator, or none.

net iperf

`net iperf client {`*`ipaddr`* `|` *`ipv6addr`* `|` *`hostname`* `[ipversion {ipv4 | ipv6}]} [port` *`port`*`] [window-size` *`bytes`*`] [data {random| default}] [interval` *`secs`*`] [{transmit-size` *`bytes`* `| duration` *`secs`*`}] [connections` *`count`*`] [nodelay]`
Starts iperf in client mode. If an IPv6 address is specified for the hostname, the `ipversion` argument must also be specified. The default is an IPv4 address. Role required: admin.

`net iperf server [run] [ipversion {ipv4 | ipv6}] [port {`*`port`* `| congestion_check-port}] [window-size` *`bytes`*`]]`
Starts iperf in server mode. The `ipversion` argument may be used to specify the type of addressing. Role required: admin.

`net iperf server start [port {`*`port`* `| congestion_check-port}] [ipversion {ipv4 | ipv6}] [window-size` *`bytes`*`]`
Runs iperf in the background in server (-s) mode. This command enables the terminal to be used for other operations, such as a network congestion check, while iperf is running. The `ipversion` argument specifies the type of addressing. Role required: admin.

`net iperf server status`
When the iperf server is running in the background (as invoked by `net_server start`), this command option displays the iperf server status and what connections the server is using. Role required: admin, security, user, backup-operator, or none.

`net iperf server stop`
When the iperf server is running in the background (as invoked by `net_server start`), this command option stops iperf. Role required: admin.

Argument Definitions

connections *count*
The `connections` argument determines how many connections to use, the number of which can improve throughput in a network environment with high loss, high latency and low bandwidth. This argument is equivalent to the Linux argument: `-p` *number*

data random
If WAN accelerators are on the network, the `data random` argument prevents artificial performance numbers from being returned. This argument is equivalent to the Linux argument: `-R`

duration *secs*
The `duration` argument indicates how many seconds the generator runs. This argument is equivalent to the Linux argument: `-t` *secs*

hostname
Equivalent to the Linux argument: `-c` *server-host*

interval *secs*
Equivalent to the Linux argument: `-j` *secs*

no delay
The `nodelay` argument eliminates the wait time between sends. This argument is equivalent to the Linux argument: `-N`

none
Equivalent to the Linux argument: `-X`

port
The `port` argument can be used to change the port number from the default 5001 to another number. Typically this is used to bypass network filters or test specific ports. This argument is equivalent to the Linux argument: `-p` *port*

transmit-size *bytes*
Equivalent to the Linux argument: `-n` *iperf-bytes*

window-size *bytes*
The `window-size` argument increases the amount of data sent at one time. This is equivalent to the Linux argument: `-w` *iperf-bytes*

net lookup

`net lookup {`*ipaddr* `|` *ipv6addr* `|` *hostname*`}`
Search DNS entries. This command may be used with IPv4 or IPv6 addresses. Role required: admin, security, user, backup-operator, or none.

net modify

`net modify` *virtual-ifname* `bonding {aggregate | failover}`
Change the behavior of the specified virtual interface from aggregate to failover for from failover to aggregate. Role required: admin.

net option

`net option show`
Display settings for network options. Role required: admin, security, user, backup-operator, or none.

net ping

`net ping {`*`ipadddr`* `|` *`ipv6addr`*`|` *`hostname`* `[ipversion {ipv4 | ipv6}]} [broadcast] [count` *`n`*`] [interface` *`ifname`*`] [packet-size` *`bytes`*`] [path-mtu {do | dont | want}] [pattern` *`pattern`*`] [numeric] [verbose]`

Verify the Data Domain system can communicate with a remote host. Role required: admin, security, user, backup-operator, or none.

Argument Definitions

broadcast
Enable pinging a broadcast address (available for IPv4 only).

count *n*
Number of pings to issue.

hostname
Can be converted into an IPv4 or IPv6 depending on the ipversion argument. If `ipversion` argument is not specified, IPv4 is used.

interface *ifname*
Name of interface to ping.

ipaddr
An IPv4 address is specified.

ipv6addr
An IPv6 address is specified.

numeric
Ping IP address not hostname.

packet-size
Set packet size.

path-mtu
Allow/disallow fragments.

pattern
Send packet with a pattern.

verbose
Display expanded output.

net reset

`net reset {domainname | searchdomains}`

Reset Data Domain system DNS servers, domain names, or host names to default settings. Requires system reboot for changes to take effect. Role required: admin.

`net reset dns`

Reset DNS list to default values. Requires system reboot for changes to take effect. Role required: admin.

`net reset hostname`

Reset hostname to default values. Requires system reboot for changes to take effect. Role required: admin.

net set

`net set {domainname` *`local-domain-name`* `| searchdomains` *`search-domain-list`*`}`

Set the domainname or searchdomains used by the Data Domain system. The default for `domainname` is the return from DHCP, or what is set by net set hostname command. The default for `searchdomain` is the `domainname` name, which is always included in the list of searchdomains. Role required: admin.

Example 74

```
# net set domainname yourcompany-ny.com
# net set searchdomains yourcompany2.com, yourcompany3.com
```

The `searchdomains` list is yourcompany-ny.com, yourcompany2.com and yourcompany3.com.

If the domain names provided cannot be resolved, a warning appears.

`net set dns` *`ipv4-ipv6-addr-list`*

Set the DNS server list using addresses for IP version 4, IP version 6, or both. Separate the IP addresses with a comma or a space. This command overwrites the current list of DNS servers. Only servers included in the most recently issued command are available to a Data Domain system. Role required: admin.

Example 75

```
# net set dns 10.0.0.1, 10.0.0.2, 10.0.0.3
The Name (DNS) server list is:
        10.0.0.1, 10.0.0.2, 10.0.0.3
```

Example 76

```
# net set dns 2100:bad:cafe:f00d::1:101 10.24.255.146
10.24.255.150
The Name (DNS) server list is:
        2100:bad:cafe:f00d::1:101, 10.24.255.146, 10.24.255.150
```

`net set hostname` *`host`*

Set the hostname of the Data Domain system. Note that some browsers may prevent logins to the host if the hostname contains an underscore. Data Domain recommends using hostnames without underscores to ensure the GUI can recognize and manage the host. Role required: admin.

Note

If the Data Domain system is using CIFS with Active Directory authentication, changing the hostname causes the Data Domain system to drop out of the domain. Use the `cifs set authentication` command option to rejoin the Active Directory domain.

Note

This command accepts domain names and validates that the domain name is made up of valid characters separated by periods. Although an IPv4 address passes the validation for a domain name, this command does not recognize the IP address as such and does not validate the IP address. This is not an issue for IPv6 addresses because they contain colon characters, which are invalid in host names.

`net set portnaming {slot-based | legacy}`
Change the port naming scheme. Role required: admin.

net show

`net show {domainname | searchdomains}`
Display the domain name or search domains used for email sent by a Data Domain system. Role required: admin, security, user, backup-operator, or none.

`net show all`
Display all networking information, including IPv4 and IPv6 addresses. Some IPv6 addresses are automatically generated and assigned to the base interface. Auto-generated IPv6 addresses are formed with a prefix (either 64 or matched to local router advertisements) and the interface MAC address. Auto-assigned addresses cannot be changed or modified. Role required: admin, security, user, backup-operator, or none.

`net show config [`*ifname*`]`
Display the configuration for a specific Ethernet interface. Exclude the keyword *ifname* to view the configuration for all Ethernet interfaces. This command shows auto-generated IPv6 addresses. Role required: admin, security, user, backup-operator, or none.

Example 77

```
# net show config
eth0a     Link encap:Ethernet  HWaddr 00:8C:FA:08:92:19
          inet addr:10.110.141.187  Bcast:10.110.143.255  Mask:255.255.248.0
          inet6 addr: 2620:0:170:1a04:28c:faff:fe08:9219/64 Scope:Global
          inet6 addr: fe80::28c:faff:fe08:9219/64 Scope:Link
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6891161 errors:0 dropped:0 overruns:0 frame:0
          TX packets:339319 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:726690965 (693.0 MiB)  TX bytes:102448918 (97.7 MiB)
```

Output Definitions

Bcast
IPv4 network broadcast address.

Collisions
Network collisions.

HWaddr
MAC address.

inet addr
IPv4 network address.

inet6 addr
IPv6 network address.

Link encap
Link encapsulation.

Mask
IPv4 network mask.

MTU
Maximum transfer unit.

RX bytes
Bytes of data received.

RX packets
Network packets received.

TX bytes
Bytes of data transmitted.

TX packets
Network packets transmitted.

txqueuelen
Transmit queue length.

`net show dns`

Display a list of DNS servers used by the Data Domain system. The final line in the output shows if the servers were configured manually or by DHCP. Role required: admin, security, user, backup-operator, or none.

Example 78

```
# net show dns
#   Server
-   -------------
1   10.24.255.146
2   10.24.255.150
3   10.110.188.5
-   -------------
Showing DNS servers configured manually.
```

`net show hardware`

Display Ethernet port hardware information from the kernel. Role required: admin, security, user, backup-operator, or none.

Example 79

```
# net show hardware
Port    Speed      Duplex    Supp Speeds   Hardware Address    Physical   Link Status
-----   --------   -------   -----------   -----------------   --------   -----------
eth0a   1000Mb/s   full      10/100/1000   00:26:9e:82:c1:d2   Copper     yes
eth0b   unknown    unknown   10/100/1000   00:26:9e:82:c1:d3   Copper     no
-----   --------   -------   -----------   -----------------   --------   -----------
```

Output Definitions

Port
The Ethernet interfaces on the system.

Speed
The actual speed at which the port processes data.

Duplex
Full or half duplex protocol.

Supp Speeds
Lists speeds the port is capable of using.

Hardware Address
The MAC address.

Physical
Copper or fibre.

Link Status
The status is `yes` if the link is active and `no` if the link is inactive.

`net show hostname`
Display the hostname of the Data Domain system. Role required: admin, security, user, backup-operator, or none.

`net show settings`
Display the registry settings for the network interfaces available on the system. Settings include the name for the physical, virtual, VLAN, and alias interfaces. The settings also indicate if an interface is enabled and if the interface information is from DHCP using IPv4 or IPv6. The IPv6 addressing scheme uses colons to separate values, and a prefix length to define the subnet. IPv4 uses periods to separate values and includes a netmask to define the subnet. A type field and additional settings such as bonding information are also included. Role required: admin, security, user, backup-operator, or none.

Example 80

```
# net show settings
port       enabled   DHCP   IP address                              netmask            type
additional setting
                                                                    /prefix
length
--------   -------   ----   ------------------------------------   ----------------   ----
------------------
eth0a      yes       ipv4   10.25.143.189*                         255.255.240.0*     n/
a
                            2620:0:170:1106:2a0:d1ff:feec:d0c5**   /
64
                            fe80::2a0:d1ff:feec:d0c5**             /
64
eth0b      yes       ipv6   (not specified)*                       (not specified)*   n/
a
                            2620:0:170:1106:2a0:d1ff:feec:d0c4**   /
64
                            fe80::2a0:d1ff:feec:d0c4**             /
64
eth1a      yes       no     2100:bad:cafe:f00d::deed:3e1a          /64                n/
a
                            fe80::21b:21ff:fe5f:e248**             /
64
eth1b      yes       no     2100:bad:cafe:f00d::deed:3e1b          /64                n/
a
                            fe80::21b:21ff:fe5f:e249**             /
64
eth1b:10   yes       no     2100:bad:dead:f00d::e4b:20             /64                n/
a
eth1c      yes       no     2100:bad:cafe:f00d::deed:3e1c          /64                n/
a
                            fe80::21b:21ff:fe5f:e24c**             /
64
eth1d      yes       no     2100:dead:f00d:cafe::deed:3e1d         /64                n/
a
                            fe80::21b:21ff:fe5f:e24d**             /
```

Example 80 (continued)

```
64
eth1d:10   yes       no     192.168.141.20                          255.255.255.0      n/
a
eth1d:100  yes       no     2100:bad:dead:f00d::e4b:100             /64                n/
a
eth1d:200  yes       no     192.168.141.200                         255.255.255.0      n/
a
eth1d:210  yes       no     2100:bad:dead:f00d::e4b:210             /64                n/
a
eth4a      no        n/a    n/a                                     n/a                n/
a
eth4b      yes       no     (not specified)                         (not specified)    n/
a
                            fe80::21b:21ff:fe52:8705**              /
64
--------   -------   ----   -------------------------------------   ----------------   ----
------------------
* Value from DHCP
** auto_generated IPv6 address
```

Output Definitions

DHCP
The DHCP configuration for the interface, which is ipv4 (enabled for IPv4), ipv6 (enabled for IPv6), disabled (no), or not applicable (n/a).

Enabled
The state of the interface, which is yes (enabled) or no (disabled).

IP address
The IPv4 and IPv6 addresses assigned to the interface. The auto-generated IPv6 addresses that begin with fe80 are link local addresses. The other auto-generated IPv6 addresses are global addresses that are created using the network and subnet advertised by routers on the interface and the MAC address of the interface.

Netmask/prefix length
The IPv4 network mask or IPv6 addresses prefix assigned to the interface.

Port
The Ethernet interfaces on the system. Interface eth1d represents the physical interface. Interface eth1d:10 is an alias interface that adds an IPv4 address to the base interface, and eth1d:100 is an alias interface that adds an IPv6 address to the same base interface.

Type
The label assigned to the interface with the `net config` *ifname* `type` command.

`net show stats [[ipversion {ipv4 | ipv6}] [all | listening] [detailed] |[ipversion {ipv4 | ipv6}] route | interfaces | statistics]`

Display network statistics. Role required: admin, security, user, backup-operator, or none.

Argument Definitions

all
Lists local client connections for the TCP and UDP protocols. Also lists client and server connections for the UNIX protocol.

detailed
Adds the associated processes for each connection.

interfaces
Displays a table of the driver statistics for each interface that is UP.

ipversion {ipv4 | ipv6}
Limits the display output to IPv4 or IPv6 addresses only. When this option is omitted, the system shows all TCP connections, including IPv4 and IPv6 addresses.

ipversion {ipv4 | ipv6}] route
Displays the route table (default is IPv4 only).

listening
Lists local server TCP connections.

statistics
Displays the statistics for IP, IP extended, ICMP, TCP, TCP extended, UDP, and UDP Lite.

net tcpdump

`net tcpdump capture` *`filename`* `[interface` *`iface`*`] [{host` *`host`* `[ipversion {ipv4 | ipv6}] | net {`*`ipaddr`* `[mask` *`mask`*`] |` *`ipv6addr`*`[/`*`prefixlength`*`]}}] [port` *`port`*`] [snaplen` *`bytes`*`]`
Capture data, and then copy the output file to another system for analysis. This command converts the options from the command line to equivalent `tcpdump` options. Output files are placed in `/ddvar/traces` where you can upload them to autosupport. A maximum of 10 output files may be retained on the system. If this limit is reached, you are prompted to delete some of the files. Role required: admin.

DD OS Linux Equivalent Arguments for net tcpdump
The DD OS `tcpdump` command dumps network traffic output as does the Linux `tcpdump` command. Values for *bytes* may be followed by the K, M, or G to scale the value. accordingly.

DD OS *filename*
Linux `-w /ddvar/traces/tcpdump_`*`filename`*`-C 100 -W 5`

DD OS interface *iface*
Linux `-i` *`iface`*

DD OS host *host*
Linux `host` *`host`*

DD OS net *net*
Linux `net` *`net`*

DD OS mask *mask*
Linux `mask` *`mask`*

DD OS port *port*
Linux `port` *`port`*

DD OS snaplen *bytes*
Linux `-s` *`bytes`*

`net tcpdump del {`*`filename`* `| all}`
Delete output files created by the `net tcpdump capture` command. Specify a *filename* to delete files matching the pattern `/ddvar/traces/tcpdump_`*`filename`*`*`. Specify `all` to remove all `net tcpdump` output files. Role required: admin.

net troubleshooting

`net troubleshooting duplicate-ip`

Detect duplicate IP in network. Role required: admin, security, user, backup-operator, or none.

CHAPTER 22

nfs

The `nfs` command enables you to add NFS clients and manage access to a Data Domain system. It also enables you to display status information, such as verifying that the NFS system is active, and the time required for specific NFS operations.

This chapter contains the following topics:

nfs change history

There have been no changes to this command in this release.

nfs Guidelines and Restrictions

- Separate list entries by commas, spaces, or both.

nfs add

`nfs add` *`path client-list`* `[(`*`option-list`*`)]`

Add NFS clients that can access the Data Domain system. A client can be a fully qualified domain hostname, class-C IP addresses, IP addresses with netmasks or length, an IPV6 address, an NIS netgroup name with the prefix @, or an asterisk wildcard for the domain name, such as *.yourcompany.com. Role required: admin.

An asterisk by itself means no restrictions. A client added to a subdirectory under `/data/col1/backup` has access only to that subdirectory.

The *options-list* is comma or space separated, enclosed by parentheses. If no option is specified, the default options are `rw`, `root_squash`, `no_all_squash`, and `secure`.

Note

Integrity and Privacy are not supported.

NFS Options

ro
Enable read-only permission.

rw
Enable read and write permissions (default value).

root_squash
Map requests from uid or gid 0 to the anonymous uid/gid.

no_root_squash
Turn off root squashing.

Note

no_root_squash is the default value.

all_squash
Map all user requests to the anonymous uid/gid.

no_all_squash
Turn off the mapping of all user requests to the anonymous uid/gid (default value).

secure
Require that requests originate on an Internet port that is less than IPPORT_RESERVED (1024) (default value).

insecure
Turn off the secure option.

anonuid=*id*
Set an explicit user ID for the anonymous account. The ID is an integer bounded from 0 to 65635.

anongid=*id*
Set an explicit group ID for the anonymous account. The ID is an integer bounded from 0 to 65635.

log
The system will log NFS requests. This option may impact performance.

sec
Set sec equal to the following options to activate different types of authentication security options. The default for sec is sys.

sys: Allow unauthenticated connections. Select to not use authentication.

krb5: Allow authenticated connections.

Note

You can use any combination of the sec options. Security options are colon separated.

⚠ CAUTION

If authentication options (sec options) on the DDR are selected and a client tries to connect to the DDR without setting the respective setting(s) on the client, the client will be denied with an authentication failure.

Example 81

```
nfs add path client-list (sec=sys:krb5)
```

Add NFS clients for a path using all of the security options.

Example 82

```
nfs add path client-list (log)
```

Add NFS clients for which the system will log NFS requests.

Example 83

```
nfs add / backup * (sec=krb5:sys)
```

Export /backup to all users so that any client can access the mount point, and all of the security options will be activated.

Example 84

To add an NFS client with an IP address of 192.168.1.02 and read/write access to `/backup` with the secure option, enter:

```
# nfs add /data/col1/backup 192.168.1.02
```

Example 85

To add a subnet client using its IP address followed by a length and a netmask, enter:

```
# nfs add /data/col1/test-mtree 192.168.1.02/24

# nfs add /data/col1/test-mtree 192.168.1.02/255.255.255.0
```

Example 86

To add an NFS client with an IPv6 address of 2620:0:170:1a01:250:56ff:fe8d:c6ae and read/write access to /backup with the secure option, enter:

```
# nfs add /data/col1/test-mtree 2620:0:170:1a01:250:56ff:fe8d:c6ae
```

Example 87

To add a client that uses an IPv6 address followed by a prefix length, enter:

```
# nfs add /data/col1/test-mtree 2620:0:170:1a01:250:56ff:fe8d:c6ae/64
```

Note

IPv6 addresses do not use subnet masks.

Example 88

To add an NFS export for `/data/col1/test_su`

```
# nfs add /data/col1/test_su *

nfs show clients
```

```
path                client    options
------------------  -------   ---------------------------------------
/data/col1/test_su  *         (rw,no_root_squash,no_all_squash,secure)
------------------  -------   ---------------------------------------
```

To modify the `/data/col1/test_su` export by changing `rw` to `ro`, and `secure` to `insecure`:

```
nfs add /data/col1/test_su * (ro,insecure)
```

Note

You must include a space between the client (in this case "*") and the opening parenthesis.

```
nfs show clients
```

```
path                client   options
------------------  -------  ---------------------------------------
```

Example 88 (continued)

```
/data/col1/test_su    *       (ro,no_root_squash,no_all_squash,insecure)
------------------    -------  ------------------------------------------
```

nfs del

`nfs del` *`path client-list`*
Delete specific directories, including a backup subdirectory, for one or more clients. The *client-list* can contain IPv4 and IPv6 addresses, hostnames, or an asterisk that represents all clients. Role required: admin.

Example 89

To delete an NFS client with an IP address of 192.168.1.01 from the `/ddvar` directory, enter:

```
# nfs del /ddvar 192.168.1.01
```

Example 90

To delete an NFS client with an IPv6 address of 2620:0:170:1a01:250:56ff:fe8d:c6ae from the /ddvar directory, enter:

```
# nfs del /ddvar 2620:0:170:1a01:250:56ff:fe8d:c6ae
```

nfs disable

`nfs disable`
Disable all NFS clients. Role required: admin.

nfs enable

`nfs enable`
Allow all NFS-defined clients to access the Data Domain system. Role required: admin.

nfs reset

`nfs reset clients`
Removes the existing client/share configuration, resetting the client list to the factory default (empty). In non-interactive mode, for example when the command is run as part of a script, the system will not pause. However, in interactive mode, the command warns the user and asks for confirmation before proceeding. NFS clients can access the Data Domain system when the client list is empty. Role required: admin.

Note

In interactive mode, the system will prompt the user with the following warning message:

```
This command will delete all exports and client configurations.
Do you want to proceed? (yes|no) [no]
```

`nfs reset stats`
Clear the NFS statistics. Role required: admin.

nfs show

`nfs show active`
List clients active in the past 15 minutes and the mount path for each. Role required: admin, user, backup-operator, security.

Note

The NFS data path security feature filters the Linux 'showmount' output on the client to match the client permissions in the export list. The system displays only the client's activity.

`nfs show clients`
Lists NFS clients allowed to access the Data Domain system and the mount path as well as NFS options for each. A client added using a hostname is displayed using the client's hostname. Security options and the log option are displayed for each mount point. If client is added using a hostname, and both sides support IPv6 and IPv4, then the client can connect using both addresses. Role required: admin, user, backup-operator, security.

Note

The NFS data path security feature filters the Linux 'showmount' output on the client to match the client permissions in the export list. The system does not display output that is not relevant to the client.

`nfs show detailed-stats`
Display NFS cache entries and status to facilitate troubleshooting. Role required: admin, user, backup-operator, security.

`nfs show histogram`
Display NFS operations in a histogram. Users with user role permissions may run this command. Role required: admin, user, backup-operator, security.

Output Definitions

mean (ms)
The mathematical mean time for completion of the operations.

std-dev
The standard deviation for time to complete operations, derived from the mean time.

max
The maximum time taken for a single operation.

min
The minimum time taken for a single operation.

2ms
The number of operations that took 2 ms or less.

4ms
The number of operations that took between 2ms and 4ms.

6ms
The number of operations that took between 4ms and 6ms.

8ms
The number of operations that took between 6ms and 8ms.

10ms
The number of operations that took between 8ms and 10ms.

100ms
The number of operations that took between 10ms and 100ms.

1s
The number of operations that took between 100ms and 1 second.

10s
The number of operations that took between 1 second and 10 seconds.

›10s
The number of operations that took over 10 seconds.

`nfs show port`
Display NFS port information. Role required: admin, user, backup-operator, security.

`nfs show stats`
Display NFS statistics. Role required: admin, user, backup-operator, security.

nfs status

`nfs status`
Enter this option to determine if the NFS system is operational. When the filesystem is active and running, the output shows the total number of NFS requests since the filesystem started, or since the last time that the NFS statistics were reset.

CHAPTER 23

ntp

The `ntp` command synchronizes a Data Domain system with an NTP time server, manages the NTP service, or turns off the local NTP server.

A Data Domain system can use a time server supplied through the default multicast operation, received from Dynamic Host Configuration Protocol (DHCP), or set manually with the Data Domain system `ntp add` command.

This chapter contains the following topics:

ntp Change History

There have been no changes to this command since the 5.4 release.

ntp Guidelines and Restrictions

- Default system settings for NTP service are enabled and multicast.
- Time servers set with the `ntp add` command override time servers from DHCP and from multicast operations.
- Time servers from DHCP override time servers from multicast operations.
- The Data Domain system `ntp del` and `ntp reset` commands act only on manually added time servers, not on DHCP-supplied time servers. You cannot delete DHCP time servers or reset to multicast when DHCP time servers are supplied.

ntp add

`ntp add timeserver` *`server-name`*
Add a remote time server to NTP list. Role required: admin. This command option requires security officer authorization for Retention Lock Compliance systems.

Example 91

To add an NTP time server named srvr26.yourcompany.com to the list, enter:

```
# ntp add timeserver srvr26.yourcompany.com
```

ntp del

`ntp del timeserver` *`server-name`*
Delete a manually added time server from the list. Role required: admin. This command option requires security officer authorization for Retention Lock Compliance systems.

Example 92

To delete an NTP time server named srvr26.yourcompany.com from the list, enter:

```
# ntp del timeserver srvr26.yourcompany.com
```

ntp disable

`ntp disable`
Disable NTP service on a Data Domain system. Role required: admin. This command option requires security officer authorization for Retention Lock Compliance systems.

ntp enable

`ntp enable`

Enable NTP service on a Data Domain system. Role required: admin. This command option requires security officer authorization for Retention Lock Compliance systems.

ntp reset

`ntp reset`

Reset the NTP configuration to the default settings. Role required: admin. This command option requires security officer authorization for Retention Lock Compliance systems.

`ntp reset timeservers`

Reset the time server list from manually entered time servers to DHCP time servers (if supplied) or to the multicast mode (if no DHCP time servers supplied). Role required: admin. This command option requires security officer authorization for Retention Lock Compliance systems.

ntp show

`ntp show config`

Display status of NTP: enabled or disabled, and show the time server list. Role required: admin, security, user, backup-operator, or none.

ntp status

`ntp status`

Display the local NTP service status, time, and synchronization information. Role required: admin, security, user, backup-operator, or none.

CHAPTER 24

quota

The `quota` command lets you modify the amount of storage space for MTrees and for VTL and DD Boost storage units. There are two quota limits: hard and soft. The hard limit prevents writes from exceeding the quota. An error message is issued if the hard limit is exceeded. The soft limit allows writes to exceed the quota. However, an alert is generated if this happens. The soft limit value must be less than the hard limit value. Quota limit values must be specified as integers.

You can set a hard limit, a soft limit, or both, depending on your requirements. For example, an administrator may choose to enforce only a soft limit to prevent overnight backup jobs from failing when the quota limit is reached. Or the administrator may choose to enforce only a hard limit to block a user from writing when the quota limit is reached.

Snapshots capture quota information at a precise point in time. Usage tracking in the active file system does not account for the space of a snapshot, so quota limits are not enforced on snapshots.

This chapter contains the following topics:

quota Change History

This section provides a list of changes since the 5.4 release, for all 5.5.x releases, in order of the most recent release to the first release.

New Commands in DD OS 5.5

`quota capacity`
Disables capacity quota, and also disables MTree quota limits and restores the limits to the default state.

`quota streams`
Resets streams quota soft-limits.

Deprecated Commands in DD OS 5.5

`quota disable`
See `quota capacity disable`.

`quota enable`
See `quota capacity enable`.

`quota reset`
See `quota capacity reset`.

`quota set`
See `quota capacity set`.

`quota show`
See `quota capacity show`.

`quota status`
See `quota capacity status`.

Note

The new `quota capacity` command also includes the new commands `quota capacity disable`, `quota capacity enable`, `quota capacity reset`, `quota capacity set`, `quota capacity show`, and `quota capacity status`.
The new `quota streams` command also includes the new commands `quota streams reset storage`, `quota streams set storage-units`, and `quota streams show`.

---

quota Guidelines and Restrictions

- MTree quotas with a hard limit cannot be set on the `/data/col1/backup` directory.
- The maximum MTree quota value is 4096 PiB. See the `mtree` command for more detail.

quota capacity

`quota capacity disable`

Disable capacity quota. Also disables MTree quota limits and restores the limits to the default state (unlimited).

Role required: admin.

`quota capacity enable`
Enable capacity quota.

Role required: admin.

`quota capacity reset { all | mtrees` *`mtree-list`* `| storage-units` *`storage-unit-list`* `} [soft-limit] [hard-limit]`
Reset capacity quota limits. If hard or soft limits are not entered, both are reset to the default state (unlimited).

Role required: admin.

To reset hard and soft limits for an MTree:

```
# quota capacity reset mtrees /data/col1/backup1
```

To reset only a soft limit for an MTree:

```
# quota capacity reset mtrees /data/col1/backup1 soft-limit
```

To reset only a hard limit for an MTree:

```
# quota capacity reset mtrees /data/col1/backup3 hard-limit
```

To reset hard and soft limits for a storage-unit:

```
# quota capacity reset storage-units DDBOOST_STRESS_SU
```

`quota capacity set {all | mtrees` *`mtree-list`* `| storage-units` *`storage-unit-list`*`} {soft-limit` *`n`* `{MiB|GiB|TiB|PiB} | hard-limit` *`n`* `{MiB|GiB|TiB|PiB} | soft-limit` *`n`* `{MiB|GiB|TiB|PiB} hard-limit` *`n`* `{MiB|GiB|TiB|PiB}}`
Set capacity quota limits during runtime for multiple MTrees. When used for storage units, this command option sets limits only after the storage unit is created. Note that the quota feature must be enabled, because limits are otherwise not enforced. Setting quotas does not require disabling the file system and therefore does not affect system performance.

Role required: admin.

To set a soft limit quota of 10 GiB on MTree `/data/col1/backup1` when the quota feature is disabled:

```
# quota capacity set mtrees /data/col1/backup1 soft-limit 10 GiB
```

To set a hard limit quota of 10 TiB on MTree `/data/col1/backup1`:

```
# quota capacity set mtrees /data/col1/backup1 hard-limit 10 GiB
```

To set a soft limit quota of 100 GiB and a hard limit quota of 1 TiB on MTree `/data/col1/backup1`:

```
# quota capacity set mtrees /data/col1/backup1 soft-limit 10 GiB hard-limit 10 TiB
```

To set a soft limit quota of 100 GiB and a hard limit quota of 1 TiB on storage-unit DDBOOST_STRESS_SU:

```
# quota capacity set storage-units DDBOOST_STRESS_SU soft-limit 100 GiB hard-limit 1 TiB
```

`quota capacity show {all | mtrees` *`mtree-list`* `| storage-units` *`storage-unit-list`* `| tenant-unit` *`tenant-unit`*`}`
List capacity quotas and usage of a particular mtree or storage unit, all mtrees or storage units, or all of both. The unit of display for usage and limits is MiB.

Role required: admin, security, user, backup-operator, none, tenant-admin, tenant-user.

`quota capacity status`
Display status of capacity quota enforcement: enabled or disabled. If output includes a note stating status as disabled, capacity quota limits are not being enforced and are therefore unlimited.

Role required: admin, security, user, backup-operator, none.

quota disable

`quota disable - deprecated`
This command is deprecated. Use `quota capacity disable` instead.

Role required: admin.

quota enable

`quota enable - deprecated`
This command is deprecated. Use `quota capacity enable` instead.

Role required: admin.

quota reset

`quota reset - deprecated`
This command is deprecated. Use `quota capacity reset` instead.

Role required: admin.

quota set

`quota set - deprecated`
This command is deprecated. Use `quota capacity set` instead.

Role required: admin.

quota show

`quota show - deprecated`
This command is deprecated. Use `quota capacity show` instead.

Role required: admin, security, user, backup-operator, none, tenant-admin, tenant-user.

quota status

`quota status - deprecated`
This command is deprecated. Use `quota capacity status` instead.

Role required: admin, security, user, backup-operator, none.

quota streams

`quota streams reset storage-units` *`storage-unit-list`* `[write-stream-soft-limit] [read-stream-soft-limit] [repl-stream-soft-limit] [combined-stream-soft-limit]`
Reset streams quota soft limits. Note that this command controls the same stream limits as `ddboost storage-unit modify`.

Role required: admin.

Example 93

```
# quota streams reset storage-units su1 write-stream-soft-limit read-stream-soft-limit repl-stream-soft-limit combined-stream-soft-limit

su1: Stream soft limits: write=none, read=none, repl=none, combined=none
```

`quota streams set storage-units` *`storage-unit-list`* `[write-stream-soft-limit` *`n`* `] [read-stream-soft-limit` *`n`* `] [repl-stream-soft-limit` *`n`* `] [combined-stream-soft-limit` *`n`* `]`
Set streams quota soft limits. Note that this command controls the same stream limits as `ddboost storage-unit modify`.

Role required: admin.

Example 94

```
# quota streams set storage-units su1 write-stream-soft-limit 10 read-stream-soft-limit 3 repl-stream-soft-limit 10 combined-stream-soft-limit 10

su1: Stream soft limits: write=10, read=3, repl=10, combined=10
```

`quota streams show {all | storage-unit` *`storage-unit`*`}`
List streams quotas for all storage units or just one storage unit.

Role required: admin, security, user, backup-operator, none.

Example 95

Example 95 (continued)

```
# quota streams show all

Storage Unit Write Streams Read Streams Repl Streams Combined Streams
               Soft-Limit   Soft-Limit   Soft-Limit     Soft-Limit
------------ ------------- ------------ ------------ ----------------
su1               10             3           10              10
su2              none           none        none            none
------------ ------------- ------------ ------------ ----------------

DD System Stream Limits: write=20 read=16 repl-in=20 repl-out=20
combined=30
```

Example 96

```
# quota streams show all

Storage Unit Write Streams Read Streams Repl Streams Combined Streams
               Soft-Limit   Soft-Limit   Soft-Limit     Soft-Limit
------------ ------------- ------------ ------------ ----------------
su1               none          none          none           none
su2               none          none          none           none
------------ ------------- ------------ ------------ ----------------

DD System Stream Limits: write=20 read=16 repl-in=20 repl-out=20
combined=30
```

CHAPTER 25

replication

EMC Data Domain Replicator lets you replicate data (copy and synchronize) between two Data Domain systems: a source and a destination. Source and destination configurations, or pairs, are also known as “contexts.” Depending on your objective, you can replicate entire sites, specific directories, MTrees, or files within a VTL (virtual tape library). Replication is a licensed software option. See the *EMC Data Domain Operating System Administration Guide* for details on replication practices and procedures.

This chapter contains the following topics:

replication Change History

This section provides a list of changes since the 5.4 release, for all 5.5.x releases, in order of the most recent release to the first release.

New Commands in DD OS 5.5

`replication throttle show performance`
Shows current throttle throughput for an optionally specified number of times and interval.

Modified Arguments in DD OS 5.5

`replication show detailed-history ... [duration hr] [interval hr]`
Arguments `duration` and `interval` can now be specified only in hours, instead of hours and/or minutes.

`replication show history ... [duration hr] [interval hr]`
Arguments `duration` and `interval` can now be specified only in hours, instead of hours and/or minutes.

`replication throttle add`
New argument `destination` *host* specifies throttle when only a few destinations need to be throttled, or when a destination requires a setting different from the default throttle.

`replication throttle del`
New argument `destination` *host* specifies throttle when only a few destinations need to be throttled, or when a destination requires a setting different from the default throttle.

`replication throttle reset`
New argument `destination` *host* specifies throttle when only a few destinations need to be throttled, or when a destination requires a setting different from the default throttle.

`replication throttle set current`
New argument `destination` *host* specifies throttle when only a few destinations need to be throttled, or when a destination requires a setting different from the default throttle.

`replication throttle set override`
New argument `destination` *host* specifies throttle when only a few destinations need to be throttled, or when a destination requires a setting different from the default throttle.

`replication throttle show`
New argument `destination` *host* specifies throttle when only a few destinations need to be throttled, or when a destination requires a setting different from the default throttle.

Modified Output in DD OS 5.5

replication show detailed-history ... [duration *hr*] [interval *hr*]

Output of `duration` and `interval` is now shown only in hours, instead of hours and/or minutes.

Also, new column, `Replicated Post-synthetic-optim`, indicates the number of bytes still needed to send/receive after the optimization for synthetic backup-aware replication is applied.

replication show detailed-stats

New column, `Bytes after synthetic optimization`, indicates the number of bytes still needed to send/receive after the optimization for synthetic backup-aware replication is applied.

replication show history ... [duration *hr*] [interval *hr*]

Output of `duration` and `interval` is now shown only in hours, instead of hours and/or minutes.

replication watch

Output, in general, is more intuitive, with better labeling and percentage indicators.

replication Guidelines and Restrictions

- When entering source names that include spaces or special characters, enclose the entire source pathname with double quotation marks, or enter a backslash before the space, but do not use both.
- Command options may take several seconds to conclude when a Data Domain system is at, or near, capacity.

replication abort

`replication abort recover` *`destination`*

Stop a recover process. Run this on the destination Data Domain system only. Then, reconfigure replication on the source Data Domain system and restart the recover process.

Role required: admin.

`replication abort resync` *`destination`*

Stop a resync operation. Run this on the source or destination Data Domain system.

Role required: admin.

replication add

`replication add source` *`source`* `destination` *`destination`* `[low-bw-optim {enabled | disabled}] [encryption {enabled | disabled}] [propagate-retention-lock {enabled | disabled}] [ipversion {ipv4 | ipv6}]`

Create a replication pair, which can be for MTree, Directory, or Collection Replication. If the *destination* exists, you will get an error, and you must either delete it or rename it before proceeding.

If a source or destination name does not correspond to a Data Domain network name, run `replication modify connection-host` on the source system. When entering

names that include spaces or special characters, enclose the entire pathname with double quotation marks, or enter a backslash before the space, but do not use both.

A file or a directory may not be renamed or moved into or out of a source. This includes a "cut" operation followed by a "paste" operation in Windows.

After replication is initialized, ownership and permissions of the destination are always identical to those of the source. If the context is configured, the destination is kept in a read-only state and can receive data only from the source.

Role required: admin.

Some Notes about Collection Replication:

- The storage capacity of the destination system must be equal to, or greater than, that of the source system. If the destination capacity is less than that of the source, the available capacity on the source is reduced to that of the destination.
- The destination must have been destroyed and subsequently created, but not enabled.
- Each destination and each source can be in only one context at a time.

Some Notes about MTree Replication:

- You can "reverse" the context for an MTree Replication, that is, you can switch the destination and the source.
- Subdirectories within an MTree cannot be replicated, because the MTree, in its entirety, is replicated.
- MTree Replication is supported from Extended Retention systems to non-Extended Retention systems if both are running DD OS 5.5.

Some Notes about Directory or MTree Replication:

- The destination Data Domain system must have available storage capacity of at least the post-compressed size of the expected maximum post-compressed size of the source directory or MTree.
- When replication is initialized, a destination directory is created automatically.
- A Data Domain system can simultaneously be the source for one context and the destination for another context.

Example 97 Collection Replication

In this example, notice the prefix **col** to the URL signifying Collection Replication. The source hostname is **system-dd1**, and the destination hostname is **system-dd2**.

```
# replication add source col://system-dd1.chaos.local destination
col://system-dd2.chaos.local
```

Example 98 MTree Replication

In this example, notice the prefix **mtree** to the URL signifying MTree Replication. The source MTree path is **/data/col1/mtree1**, and the destination MTree path is **/data/col1/dstmtree1**.

```
# replication add source mtree://system-dd1.chaos.local/data/col1/
mtree1 destination mtree://system-dd2.chaos.local/data/col1/dstmtree1
```

Example 99 Directory Replication

In this example, notice the prefix **dir** to the URL signifying Directory Replication. The source directory name is **dir1**, and it resides in the **/backup** MTree (the default MTree).

```
# replication add source dir://system-dd1.chaos.local/backup/dir1
destination dir://system-dd2.chaos.local/backup/dir1
```

Argument Definitions

low-bw-optim {enabled | disabled}
Enables or disables *low bandwidth optimization*, which improves data transfer over low bandwidth links by adding increased data compression to optimize network bandwidth. Both the source and the destination must enable this feature.

Low bandwidth optimization is not supported if the DD Extended Retention software option is enabled on either Data Domain system. It is also not supported for Collection Replication.

encryption {enabled | disabled}
Enables or disables *encryption over wire*. Both the source and the destination must enable this feature. Encrypted replication uses the ADH-AES256-SHA cipher suite.

propagate-retention-lock {enabled | disabled}
Enables or disables the propagation of Retention Lock. This cannot be enabled for Directory Replication.

ipversion {ipv4 | ipv6}
Lets you choose your network preference for the replication pair. An IPv6-enabled replication service can still accept connections from an IPv4 replication client if the service is reachable via IPv4. An IPv6-enabled replication client can still communicate with an IPv4 replication service if the service is reachable via IPv4.

replication break

`replication break {`*`destination`* `| all}`

Remove the source or destination Data Domain system from a replication pair, or remove all Replicator configurations from a Data Domain system.

Role required: security for Retention Lock Compliance systems; admin for all other systems.

replication disable

`replication disable {`*`destination`* `| all}`

Run this on the source or destination system to halt data replication temporarily. If run on the source, the operation stops sending data to the destination. If run on the destination, the operation stops serving the active connection from the source.

Role required: security for Retention Lock Compliance systems: admin for all other systems.

replication enable

`replication enable {`*`destination`* `| all}`

Restart replication. If run on the source, the operation resumes sending data to the destination. If run on the destination, the operation resumes serving the active connection from the source.

Role required: admin.

replication initialize

`replication initialize` *`destination`*

Run this on the source to start replication between a source and destination and to verify that the configuration and connections are correct. Error messages are returned if problems appear.

Initialization can take several hours, or days, depending on the amount of data in the source. To reduce initialization time, consider placing both Data Domain systems of the replicator pair in the same location with a direct link. The *destination* variable is required.

Key-manager settings on a destination are ignored when users set up and initialize a collection replication pair. The keys are copied to the replica, but key-manager settings are not. If the destination is configured with key-manager settings prior to becoming the replication destination, the settings remain on the system but are not used. If a collection replication breaks, you must reconfigure the destination to use the correct key-manager settings and key class.

EMC recommends resetting the key-manager on the destination prior to collection replication, and then configuring the destination with the correct key manager-server and key class after a collection replication is broken.

Role required: admin.

replication modify

`replication modify` *`destination`* `connection-host` *`new-host-name`* `[port` *`port`*`]`

Modify the destination host name, when it does not resolve for the connection, to a new host name or IP address. You may also specify an optional port number. This action may be required when a connection passes through a firewall. It is definitely required when connecting to an alternate listen-port on the destination. It may also be required after adding a new source and destination pair, or after renaming a source or a destination. Role required: admin.

`replication modify` *`destination`* `{source-host | destination-host}` *`new-host-name`*

Modify the source or destination host name. In this case, you must modify the replication configuration on both the source and the destination; that is, if the host name that changed was the destination, you must run replication modify on both the destination and the source so both sides will be updated. The *new-host-name* must be the name returned by `net show hostname` on the system receiving the new host. When using `replication modify`, always run `filesys disable` or `replication disable` first, and conclude with `filesys enable` or `replication enable`. Then, run `replication show config` to make sure all changes were done. Role required: admin.

Example 100

If local destination ca.company.com is moved from California to New York, run the following on both the source and the destination:

Example 100 (continued)

```
# replication disable
# replication modify dir://ca.company.com/backup/dir2 destination-
host ny.company.com
# replication enable
# replication show config
```

`replication modify` *`destination`* `encryption {enabled | disabled}`
Modify the state of encryption over wire for the destination. This feature is active only when enabled on both the source and the destination. Role required: admin.

`replication modify` *`destination`* `ipversion {ipv4 | ipv6}`
Modify the network preference for the destination. An IPv6-enabled replication service can still accept connections from an IPv4 replication client if the service is reachable via IPv4. An IPv6-enabled replication client can still communicate with an IPv4 replication service if the service is reachable via IPv4. Role required: admin.

`replication modify` *`destination`* `low-bw-optim {enabled | disabled}`
Modify the state of low bandwidth optimization for the destination. This feature is active only when enabled on both the source and the destination. This feature is not supported for collection replication or if DD Extended Retention is enabled on either the source or the destination. Role required: admin.

replication option

`replication option reset {bandwidth | delay | listen-port | default-sync-alert-threshold}`
Reset system bandwidth, delay, listen port, and sync-alert-threshold to default values.

Defaults are `bandwidth`, unlimited; `delay`, none; `listen-port`, 2051. Default for `sync-alert-threshold` is 24 (hours).

When using `replication option reset`, always run `filesys disable` first, and conclude with `filesys enable`.

Role required: admin.

`replication option set bandwidth` *`rate`*
Set the network bandwidth rate for the Data Domain system. You must set the bandwidth and network delay on each side of the connection.

Role required: admin.

`replication option set default-sync-alert-threshold` *`value`*
Set the sync time to configure when an alert is generated. The sync time is set in hours. The default *value* is 24.

Role required: admin.

`replication option set delay` *`value`*
Set the network delay in milliseconds for the Data Domain system. You must set the bandwidth and network-delay on each side of the connection.

Role required: admin.

`replication option set listen-port` *`value`*
Set the listen port for the Data Domain system. On a destination Data Domain system, set the port from which the destination receives data from replication sources (the default is

2051). A destination can have only one listen port used by all sources. The connection-host port used by a source must match the listen port used by the destination.

For DD Boost managed file replication, the listen port is used on the source Data Domain system and on the destination Data Domain system to specify the connection-host port. For directory replication, `replication modify connection-host` is used on the source Data Domain system.

Role required: admin.

`replication option show`
Display the current bandwidth, network-delay settings, listen port, and sync-alert-threshold. If these settings are configured using default values, `replication option show` returns a command prompt with no setting information.

Role required: admin, security, user, backup-operator, none.

replication reauth

`replication reauth` *`destination`*
Resets authentication on the source and destination systems. The *destination* variable is required. Messages similar to `Authentication keys out of sync` or `Key out of sync` indicate a reset is required. Reauthorization is primarily used when replacing a source Data Domain system.

Role required: admin.

replication recover

`replication recover` *`destination`*
Run this on a new source to move data from a destination system. If configuring collection replication, this must be run on the new source only. The *destination* argument is required. This is not available for MTree replication.

When using `replication recover`, always run `filesys disable` first, and conclude with `filesys enable`.

If `replication break` was previously run, the destination cannot be used to recover a source. If configuring directory replication, the destination directory on the source must be empty.

Role required: admin.

replication resync

`replication resync` *`destination`*
Bring back into sync (or recover) the data between a source and destination replication pair after a manual break. The replication pair are resynchronized so both endpoints contain the same data. Resynchronization is available for Directory, MTree or Pool Replication, but not for Collection Replication.

Before running `replication resync`, you must run `replication add` to add the source and destination back on the system.

A replication resynchronization can also be used:

- To recreate a context that has been deleted.
- When a destination runs out of space, but the source still has data to replicate.

- To convert a Directory Replication pair to an MTree Replication pair.

Note the following about using `replication resync` with DD Retention Lock:

- If the destination MTree or directory contains retention-locked files that do not exist on the source, then resync will fail.
- If the destination directory has retention lock enabled, but the source directory does not have retention lock enabled, then a resync of a directory replication will fail.
- With MTree replication, resync will succeed if the source MTree does not have retention lock enabled while the destination MTree has retention lock enabled or vice versa, as long as the destination MTree does not contain retention-locked files not present on the source.

Role required: admin.

replication show

`replication show config [`*`destination`* `| all]`
Show replication configuration.

Role required: admin, security, user, backup-operator, none.

`replication show detailed-history {`*`obj-spec-list`* `| all}`
`[duration` *`hr`*`] [interval` *`hr`*`]`
Show details of replication performance history.

Role required: admin, security, user, backup-operator, none.

Output Definitions

CTX
The context number, which will be zero (0) for collection replication.

Source
The Data Domain system that receives data from backup applications.

Destination
The Data Domain system that receives data from the replication source Data Domain system.

Connection Host and Port
A source system connects to the destination system using the name returned by the hostname command on the destination. It may also connect using a destination name or IP address and port designated by `replication modify connection-host`. The destination hostname may not resolve to the correct IP address when connecting to an alternate interface on the destination, or when passing through a firewall.

Low-bw-optim
The status of low-bandwidth optimization: enabled, disabled, or configuration mismatch.

Enabled
The replication process is enabled and available to replicate data (“yes”) or disabled and not available to replicate data (“no”).

Replicated Post-synthetic-optim
The number of bytes still needed to send/receive after the synthetic replication optimization is applied.

`replication show detailed-stats [`*`destination`* `| all]`
Display cumulative statistics beginning from when the context was created. This command option provides byte-count statistics related to identity filtering, delta

compression, and local compression. The ratio of the values Bytes after filtering by destination to Bytes after low bandwidth optimization gives additional compression ratio supplied by delta compression.

Role required: admin, security, user, backup-operator, none.

Output Definitions

Network bytes sent to destination
: The number of physical bytes sent to the destination over the wire.

Pre-compressed bytes written to source
: The number of logical bytes ingested to the source corresponding to the CTX.

Pre-compressed bytes sent to destination
: The number of logical bytes sent to the destination system.

Bytes after synthetic optimization
: The number of bytes still needed to send/receive after the synthetic replication optimization is applied.

Bytes after filtering by destination
: The number of bytes sent after identity filtering (dedup).

Bytes after low bandwidth optimization
: The number of bytes sent after delta compression (low-bandwidth optimization).

Bytes after local compression
: The number of bytes sent to the destination after local compression.

Pre-compressed bytes remaining
: The amount of pre-compressed data replicated.

Compression ratio
: The ratio of the value of logical bytes ingested to the source to physical bytes actually sent to the destination over the wire.

`replication show history {`*`obj-spec-list`*` | all} [duration `*`hr`*`] [interval `*`hr`*`]`

Show replication performance history. Statistics are generated hourly.

Role required: admin, security, user, backup-operator, none.

Output Definitions

Pre-Comp (KB) Remaining
: The amount of pre-compression data not replicated.

Replicated (KB) Pre-Comp
: The amount of pre-compressed data replicated.

Replicated (KB) Network
: The amount of compressed data sent over the network.

Synced-as-of Time
: The time when the most recently replicated data on the destination was generated on the source. A value of unknown appears during replication initialization.

Low-bw-optim
: The additional compression ratio supplied by delta compression (low-bandwidth optimization.

`replication show performance {`*`obj-spec-list`*` | all} [interval `*`sec`*`] [count `*`count`*`]`

Display current replication activity. Default interval is two seconds.

If a single source context is specified, four additional columns are presented. These columns show the relative amounts of time spent working on, or waiting for, replication

sender threads for the specified context. Values are calculated by the amount of time spent for the activity, multiplying the time by 100, and dividing the time by the duration of the reporting interval. Values can exceed 100 due to the presence of multiple threads working on behalf of the specified replication context.

When a replication throttle is configured, you may see a large amount of output followed by a period of none while viewing performance or statistics. This behavior is the result of how statistics are calculated by replication, combined with the default Data Domain system replication configuration of using large TCP buffers. When a throttle is in effect, data is buffered before being sent on the network.

Users may configure the replication bandwidth and delay arguments in `replication option reset` on the source and destination to use smaller TCP socket buffers. This reduces the total amount of data on the network, increases how often replication writes data to its sockets, and, as a result, increases the frequency of updates for statistics counters.

Role required: admin, security, user, backup-operator, none.

Output Definitions

Pre-comp (KB/s)
The size value before compression is applied. Sometimes referred to as *logical size*.

Network (KB/s)
The amount of compressed data transferred over the network per second.

Streams
An internal system resource associated with reads and writes. One replication context can use multiple streams for better performance.

Reading
The time spent reading file system data from the local file system. This number is typically the second highest number after Network. On a deployment with high network bandwidth, Reading may be the largest column.

Meta
The time spent on miscellaneous bookkeeping activities and replicating file system namespace operations. This value is typically under 50. If this value exceeds 50 on a sustained basis, it may indicate an unusual workload (a large number of file attribute updates, for example).

Dest
The time spent waiting because the receiver is not providing the sender enough information on what data to send. Typically this value is low. Exceptions include systems on high-speed networks where the sender is a more powerful Data Domain system than the replica, or where the replica has a higher workload than the sender because the replica is the destination for multiple replication contexts.

Network
The time spent sending file data and metadata and waiting for replies from the server on what data needs to be sent. This is typically the highest of the four values. This value exceeds 100 regularly if the sender is able to replicate multiple files in parallel.

Note

If the Network column has the highest time values among Reading, Meta, Waiting, and Network, and if the Network KB/sec value is lower than expected, a network problem may be present. For example, packet loss may be causing reduced throughput.

`replication show stats [destination | all]`

Display statistics for all replication pairs or a specific destination pair. Output format is based on replication type.

In collection replication, the difference in values between Post-comp Bytes Sent and Post-comp Bytes Received is expected behavior.

Role required: admin, security, user, backup-operator, none.

Output Definitions

CTX
The context number, which will be zero (0) for collection replication.

Destination
The replication destination.

Post-comp Bytes Sent
Network data sent by the source to the destination.

Post-comp Bytes Received
The number of bytes received by the source, including logical bytes associated with the file being replicated.

Synced-as-of-Time
The time when the most recently replicated data on the destination was generated on the source. A value of Unknown appears during replication initialization.

Pre-comp Bytes Remaining
For directory replication only, this is the sum of file sizes remaining to be replicated for the context. Output includes the entire logical size of the current file being replicated. If a large file is being replicated, this number may take a lot of time to change. The number changes only after the current file finishes.

replication status

`replication status [`*`destination`* `| all] [detailed]`
Show the current status of replication. Role required: admin, security, user, backup-operator, none.

replication sync

`replication sync [and-verify] [`*`destination`*`]`
Synchronize replication between the source and destination and wait for replication to complete. You must first configure the source and destination and initialize the context.

Role required: admin, security, backup-operator.

replication throttle

`replication throttle add [destination `*`host`* `| default] `*`sched-specrate`*
Change the rate of network bandwidth used by replication. By default, network bandwidth use is unlimited, meaning it continuously runs as fast as possible. If you set a throttle, replication runs at the given rate until the next scheduled change, or until new throttle command options force a change. Throttle is usually set at the source Data Domain system, but can optionally be set at the destination.

Role required: admin.

To limit replication to 5 megabits per second for a destination Data Domain system named ddr1-ny, starting on Tuesdays and Fridays, at 10:00 a.m., enter:

```
# replication throttle add destination ddr1-ny tue fri 2200 5Mbps
```

`replication throttle del [destination` *`host`* `| default]` *`sched-spec`*
Remove one or more throttle schedule entries.

Role required: admin.

To remove an entry for Mondays at 1:00 p.m., enter:

```
# replication throttle del mon 1300
```

`replication throttle reset [destination` *`host`* `| default] {current | override | schedule | all}`
Reset a throttling schedule.

Role required: admin.

`replication throttle set current [destination` *`host`* `| default]` *`rate`*
Set the throttle rate until the next scheduled change or a system reboot. Setting the throttle to current cannot be done if `replication throttle set override` is in effect.

Role required: admin.

`replication throttle set override [destination` *`host`* `| default]` *`rate`*
Set the throttle rate until another `override` is issued. Throttle override cannot be set if `replication throttle set current` is in effect.

Role required: admin.

`replication throttle show [destination` *`host`* `| default | all]`
Show throttle configuration. If no option is specified, *all* is the default option.

Role required: admin, security, user, backup-operator, none.

`replication throttle show performance [destination` *`host`* `| default | all] [interval` *`sec`*`] [count` *`count`*`}`
Show current throttle throughput for an optionally specified number of times and interval. If no option is specified, *all* is the default option.

Role required: admin, security, user, backup-operator, none.

To specify that results be shown exactly 7 times, at 2 second intervals (for a total of 14 seconds), enter:

```
# replication throttle show performance all interval 2 count
710/16 10:15:18
usr1-dl.datadomain
    [8000K bps]
     ---------
       (0 bps)
       (0 bps)
       (0 bps)
       (0 bps)
       (0 bps)
```

```
       (0 bps)
       (0 bps)
SE@usr1-dd1## date
Wed Oct 16 10:15:34 PDT 2013
```

Argument Definitions

all
Removes and resets current or override settings and removes all scheduled changes. This option returns the system to the default settings.

count
Specifies the number of times the results will be shown. The default is unlimited (the command will run until it is ended by the user).

current
Removes and resets the rate set by a previous `replication throttle set current`.

host
Specifies the destination hostname when you are setting up a destination throttle.

override
Removes and resets the rate set by a previous `replication throttle set override`.

rate
Specifies the rate, which can be the word `unlimited`; or a number; or disable, disabled, or zero (any of the last three will stop replication until the next rate change). If set to zero, new contexts are also throttled to zero. The system enforces a minimum rate of 98,304 bits per second (about 100 Kbps) and a maximum of 34,358,689,792 bits per second (about 34 Gbps). The number can include a tag for bits or bytes per second. Do not use a space between the number and the bits or bytes specification. The default rate is bits per second. In the rate variable:

- bps equals raw bits per second
- Kbps or kbps equals 1000 bits per second
- Mbps or mbps equals $1x10^6$ bits per second
- Gbps or gbps equals $1x10^9$ bits per second

Kib = Kibibits, the base-2 equivalent of Kb or Kilobits. KiB = Kibibytes, the base-2 equivalent of KB or Kilobytes.

sched-spec
Lets you enter one or more three-letter days of the week (such as `mon`, `tue`, or `wed`), or the word `daily` (to set the schedule every day). This argument can also specify a time of day in 24-hour format.

schedule
Removes and resets scheduled changes.

sec
Specifies the number of seconds for the interval between displaying the results. The default is five seconds.

replication watch

`replication watch` *`destination`*

Display the progress of a replication initialization, resynchronization process, or recovery operation.

Role required: admin, security, user, backup-operator, none.

During initialization:

```
# repl init rctx://14
(00:00) Initialize started.
Use 'replication watch rctx://14' to monitor progress.
# repl watch rctx://14
Use Control-C to stop monitoring.

(00:00) Replication initialize started...
(00:08) 100%: pre-initialize
(00:08) initializing 3/3:
(00:33) : 60% completed, pre-comp: 0 KB/s, network: 6 KB/s
```

When initialization completes:

```
# repl init rctx://14
(00:00) Initialize started.
Use 'replication watch rctx://14' to monitor progress.
# repl watch rctx://14
Use Control-C to stop monitoring.
(00:00) Replication initialize started...
(00:08) 100%: pre-initialize
(00:08) initializing 3/3:
(00:49) : 100% completed, pre-comp: 0 KB/s, network: 6 KB/s
(00:49) Replication initialize completed.
```

CHAPTER 26

route

The `route` command manages routing between a Data Domain system and backup hosts. An additional routing rule in the Kernel IP routing table and in the Data Domain system Route Config list shows a list of static routes reapplied at each system boot. Each interface is assigned a route based on the address assigned to it. Also, depending on the default gateway subnet, a route is added to an interface automatically if the interface is in the subnet of the default route address.

Federal certification requirements state the DD OS must be IPv6-capable and that interoperability with IPv4 be maintained in a heterogeneous environment. As a result, several net command options now include arguments for both versions of Internet Protocol. EMC Data Domain customers select which version to use, based on the type of configuration.

This chapter contains the following topics:

route Change History

There have been no changes to this command since the 5.4 release.

route Guidelines and Restrictions

- Changes to Ethernet interfaces made with `net` command options flush the routing table. All routing information is lost and data movement using routing is cut off immediately. EMC Data Domain recommends making interface changes only during scheduled downtime. You must reconfigure routing rules and gateways after making interface changes.

route add

`route add [ipversion {ipv4 | ipv6}]` *`route-spec`*
Add a routing rule. Role required: admin.

Example 101

To add a route with a route specification of 192.168.1.x, a netmask, and a gateway of srvr12, enter:

```
# route add -net 192.168.1.0 netmask 255.255.255.0 gw srvr12
```

Example 102

To add a route for host user24 with a gateway of srvr12, enter:

```
# route add -host user24 gw srvr12
```

route del

`route del [ipversion {ipv4 | ipv6}] <`*`route spec`*`>`
The IPv4 *route spec* syntax is: *ipv4address* [*netmask*] gw *gateway*

The IPv6 *route spec* syntax is: *ipv6address* gw *gateway*

Delete an IPv4 or IPv6 static route for a network or network host. Role required: admin.

Argument Definitions

gw *gateway*
Specifies the IP address of the gateway used to reach the destination network or host.

ipv4address
Specifies the IPv4 address of the destination network or host.

ipv6address
Specifies the IPv6 address of the destination network or host.

ipversion ipv4
Specifies that the route is an IPv4 route. If this is omitted, the route is deleted from the IPv4 routing table.

ipversion ipv6
Specifies that the route is an IPv6 route. If this is omitted, the route is deleted from the IPv4 routing table.

-netmask
Specifies the network mask that applies to the destination network or network host.

Example 103

To delete a route, for example, 192.168.1.0 and a netmask of 255.255.255.0, enter:

```
# route del 192.168.1.0 netmask 255.255.255.0  gw 10.25.160.
```

route reset

`route reset gateway [ipversion {ipv4 | ipv6}]`
Reset the default routing gateway to the default value (empty). Role required: admin.

route set

`route set gateway {`*`ipaddr | ipv6addr`*`}`
Change the routing default gateway. When the default gateway is added or changed, the Data Domain operating system automatically adds a route to default gateway for each interface with the same subnet. Role required: admin.

Note

When configuring an IPv6 address, a command failure might not produce an error message in the CLI. If the new gateway is not visible using the `route show gateway` and `route show table` commands, check the *messages* log file for information on why the command failed.

Example 104

To give a default gateway when no other route matches, enter:

```
# route set gateway 192.168.10.1
```

route show

`route show config`
Display the configured static routes that are in the Route Config list. Role required: admin, security, user, backup-operator, or none.

`route show gateway [ipversion {ipv4 | ipv6}]`
Display the configured or DHCP-supplied routing gateways used by a Data Domain system. Role required: admin, security, user, backup-operator, or none.

`route show table [ipversion {ipv4 | ipv6}]`

Display all entries in the Kernel IP routing table. Role required: admin, security, user, backup-operator, or none.

route trace

`route trace [ipversion {ipv4 | ipv6}] host`

Display a route used by a Data Domain system to connect with a particular destination. Role required: admin, security, user, backup-operator, or none.

Example 105

To trace the route to srvr24, enter:

```
# route trace srvr24
Traceroute to srvr24.yourcompany.com (192.168.1.6), 30 hops max, 38
byte packets
1 srvr24 (192.168.1.6) 0.163 ms 0.178 ms 0.147 ms
```

CHAPTER 27

scsitarget

The `scsitarget` command manages the SCSI (Small Computer System Interface) target subsystem configuration on single-node Data Domain systems and on systems using Extended Retention.

The SCSI target subsystem configuration comprises several SCSI target entities:

- services (VTL and DD Boost)
- transports (Fibre Channel)
- transport endpoints (Fibre Channel port)
- endpoints (such as VTL tape drives)
- logical devices
- host initiators
- access groups

This chapter contains the following topics:

scsitarget Change History

This section provides a list of changes since the 5.4 release, for all 5.5.x releases, in order of the most recent release to the first release.

Modified Arguments in DD OS 5.5

scsitarget device show detailed [*device-spec*] [service *service-name*] [group *group-spec*]
Arguments and variables *device-spec*, *service-name*, and *group-spec* now support vdisk device-specs, service, and group-specs, respectively.

scsitarget device show list [*device-spec*] [service *service-name*] [group *group-spec*]
Arguments and variables *device-spec*, *service-name*, and *group-spec* now support vdisk device-specs, service, and group-specs, respectively.

scsitarget endpoint modify ... [system-address *system-address*]
New argument `system-address` *system-address* lets you change the system-address of an endpoint.

scsitarget group add ... device *device-spec* ...
Argument `device` *device-spec* now supports vdisk device-specs.

scsitarget group attach ... device *device-spec* ...
Argument `device` *device-spec* now supports vdisk device-specs.

scsitarget group create ... service *service-name* ...
Argument `service` *service-name* now supports vdisk service.

scsitarget group del ... device *device-spec* ...
Argument `device` *device-spec* now supports vdisk device-specs.

scsitarget group detach ... device *device-name* ...
Argument `device` *device-name* now supports vdisk device-names.

scsitarget group modify ... device *device-spec* ...
Argument `device` *device-spec* now supports vdisk device-specs.

scsitarget group show detailed [*group-spec*] [device *device-spec*] ... [service *service-name*]
Arguments and variables *group-spec*, `device` *device-spec*, and `service` *service-name* now support vdisk group-specs, device-specs, and service, respectively.

scsitarget group show list [*group-spec*] [device *device-spec*] ... [service *service-name*]
Arguments and variables *group-spec*, `device` *device-spec*, and `service` *service-name* now support vdisk group-specs, device-specs, and service, respectively.

scsitarget group use [*group-name*] [device *device-spec*] ...
Argument `device` *device-spec* now supports vdisk device-specs.

scsitarget initiator show detailed ... [group *group-spec*]
Argument `group` *group-spec* now supports vdisk group-specs.

scsitarget initiator show list ... [group *group-spec*]
Argument `group` *group-spec* now supports vdisk group-specs.

scsitarget persistent-reservation clear [device *device-spec*] ...
Argument `device` *device-spec* now supports vdisk device-specs.

scsitarget persistent-reservation show detailed [device *device-spec*] ...
Argument `device` *device-spec* now supports vdisk device-specs.

scsitarget persistent-reservation show list [device *device-spec*] ...
Argument `device` *device-spec* now supports vdisk device-specs.

scsitarget service refresh [*service*]
Argument *service* now supports vdisk service.

scsitarget trace enable [service *service-name*]
Argument `service` *service-name* now supports vdisk service.

Modified Output in DD OS 5.5

scsitarget device show detailed
Output now includes information for vdisk devices.

scsitarget device show list
Output now includes information for vdisk devices.

scsitarget group show detailed
Output now includes information for vdisk devices.

scsitarget group show list
Output now includes information for vdisk devices.

scsitarget persistent-reservation show detailed
Output now includes information for vdisk devices.

scsitarget persistent-reservation show list
Output now includes information for vdisk devices.

scsitarget service show list
Output now includes information for vdisk devices.

scsitarget trace show
Output now includes information for vdisk devices.

scsitarget Guidelines and Restrictions

- In some cases, mostly group management, individual services provide interfaces tailored to the service, for example, vtl group. These may be more convenient for daily use than the generic scsitarget interface.
- Names of logical devices, endpoints, and access groups are case-insensitive and case-preserving. They cannot include colons, question marks, commas, asterisks, forward or backward slashes, or open or closed parentheses.
- Names for logical devices and endpoints cannot include the word **all**.
- Names for access groups cannot include the words **summary**, **all**, or **VTL**.

scsitarget device

`scsitarget device show detailed [`*device-spec*`] [service` *service-name*`] [group` *group-spec*`]`
Show detailed information for SCSI target or vdisk devices.

Role required: admin, security, user, backup-operator, none.

`scsitarget device show list [`*`device-spec`*`] [service `*`service-name`*`] [group `*`group-spec`*`]`
List summary information for SCSI target or vdisk devices. If no arguments are selected, the output will include basic information for all device criteria, including vdisk devices.

Role required: admin, security, user, backup-operator, none.

Argument Definitions

device-spec
A list of devices that uses wildcards. This can be a vdisk *device-spec*.

group-name
Name of SCSI target access group.

service-name
A SCSI target service: vtl, ddboost, or vdisk.

scsitarget disable

`scsitarget disable`
Disable the SCSI target subsystem.

Role required: admin.

scsitarget enable

`scsitarget enable`
Enable the SCSI target subsystem.

Role required: admin.

scsitarget endpoint

`scsitarget endpoint connection-reset `*`endpoint-spec`*
Reset one or more SCSI target endpoints. Be aware that resetting endpoint connections during a backup may disrupt the backup operation.

Role required: admin.

`scsitarget endpoint del `*`endpoint-spec`*
Delete one or more endpoints. This may be used to delete an endpoint if the underlying hardware is no longer available. If the underlying hardware is still present, or becomes available, a new endpoint for the hardware is discovered automatically and configured based on default values.

Role required: admin.

`scsitarget endpoint disable `*`endpoint-spec`*
Disable one or more SCSI target endpoints.

Role required: admin.

`scsitarget endpoint enable `*`endpoint-spec`*
Enable one or more SCSI target endpoints.

Role required: admin.

`scsitarget endpoint modify `*`endpoint-spec`*` [fcp2-retry {disable | enable | default}] [topology {loop-preferred | loop-only |`

`point-to-point | default}] [wwpn {auto | wwpn}] [wwnn {auto | wwnn}] [system-address address]`
Modify one or more endpoints.

Role required: admin.

`scsitarget endpoint rename src-endpoint-name dst-endpoint-name`
Rename an endpoint.

Role required: admin.

`scsitarget endpoint show detailed [endpoint-spec]`
Show detailed information about one or more endpoints.

Role required: admin, security, user, backup-operator, none.

`scsitarget endpoint show list [endpoint-spec]`
Show summarized list of configured endpoints. If no argument is selected, the output will be basic information for all endpoint criteria.

Role required: admin, security, user, backup-operator, none.

`scsitarget endpoint show stats [endpoint-spec] [interval interval] [count count]`
Periodically list I/O statistics on one or more endpoints. If no endpoints are specified, the output will be a single-line total for each interval.

Role required: admin, security, user, backup-operator, none.

Argument Definitions

count
The number of objects on which to perform the action, as specified by the command option.

endpoint-spec
A list of endpoints (logical names for target ports on a Data Domain system) that uses a wildcard.

fcp2-retry
Port option.

interval *interval*
Time interval in seconds. The default is 2 seconds.

system-address
The related system address of a SCSI target endpoint.

topology
Set the Fibre Channel topology for the endpoint. Values include: `loop-preferred`, `loop-only`, `point-to-point`, `default`.

wwpn
Set the worldwide port name (WWPN) for the endpoint, or use an automatic system-generated WWPN.

wwnn
Set the worldwide node name (WWNN) for the endpoint, or use an automatic system-generated WWNN.

scsitarget group

`scsitarget group add group-name device device-spec [lun lun] [primary-endpoint {all | none | endpoint-list}] [secondary-endpoint {all | none | endpoint-list}]`

Add SCSI target or vdisk devices to a group.

Role required: admin.

`scsitarget group add` *group-name* `initiator` *initiator-spec*
Add one or more initiators to a group.

Role required: admin.

`scsitarget group attach` *group-name* `device` *device-name* `lun` *lun* `primary-endpoint {all | none |` *endpoint-list*`} secondary-endpoint {all | none |` *endpoint-list*`}`
Attach an additional LUN to a SCSI target or vdisk device in a group. This may be used to expose a device with different LUNs through different endpoints.

Role required: admin.

`scsitarget group create` *group-name* `service` *service-name*
Create a new group associated with a specific service, which can be a vdisk service.

Role required: admin.

`scsitarget group del` *group-name* `device` *device-spec*
Delete one or more SCSI target or vdisk devices from a group.

Role required: admin.

`scsitarget group del` *group-name* `initiator` *initiator-spec*
Delete one or more initiators from a group.

Role required: admin.

`scsitarget group destroy` *group-name*
Destroy a group.

Role required: admin.

`scsitarget group detach` *group-name* `device` *device-name* `lun` *lun*
Detach a SCSI target or vdisk device from a LUN in a group. There must be at least one LUN for a device in a group.

Role required: admin.

`scsitarget group modify` *group-name* `device` *device-spec* `[lun` *lun*`] [primary-endpoint {all | none |` *endpoint-list*`}] [secondary-endpoint {all | none |` *endpoint-list*`}]`
Modify SCSI target or vdisk device attributes in a group. If a device is attached to multiple LUNs, the *lun* argument, if specified, indicates which LUN to update.

Role required: admin.

`scsitarget group rename` *src-group-namedst-group-name*
Rename a group.

Role required: admin.

`scsitarget group show detailed [`*group-spec*`] [device` *device-spec*`] [initiator` *initiator-spec*`] [service` *service-name*`]`
Show detailed information on specific groups, based on selected arguments.

Role required: admin, security, user, backup-operator, none.

```
#scsitarget group show detailed vdisk_g1
Group: vdisk_g1
Service: VDISK
Active state: active
```

```
Initiators: None
Devices: None
Service: VDISK
Active state: active
Address: [0/0/0] (0)
```

`scsitarget group show list [`*`group-spec`*`] [device `*`device-spec`*`] [initiator `*`initiator-spec`*`] [service `*`service-name`*`]`

Display a list of groups based on selected arguments. If no arguments are selected, output displays basic information on all group criteria, including vdisk devices.

Role required: admin, security, user, backup-operator, none.

```
# scsitarget group show list
Group Name   Service   # Initiators   # Devices
----------   -------   ------------   ---------
TapeServer       VTL              0           0
disk1          VDISK              0           0
test1            VTL              0           0
vdisk_g1       VDISK              0           0
vdisk_g2       VDISK              0           0
----------   -------   ------------   ---------
```

`scsitarget group use `*`group-name`*` device `*`device-spec`*` {primary | secondary}`

Switch the in-use endpoint lists for one or more SCSI target or vdisk devices in a group between primary and secondary endpoint lists. For best results, do not run this command option during heavy VTL usage.

Role required: admin.

Argument Definitions

all
Show all information about the object specified by the command option.

device-name
Name of the SCSI target or vdisk device.

device-spec
A list of devices that uses wildcards. This can be a vdisk *device-spec*.

group-name
Name of SCSI target access group.

group-spec
A list of access groups that uses a wildcard. This can be a vdisk *group-spec*.

initiator-spec
A list of initiators that uses a wildcard.

lun
A device address to pass to the initiator. The maximum logical unit number (LUN) is 16383. A LUN must be unique within a group, but need not be unique across the system. LUNs for VTL devices within a group must start with zero and be contiguous numbers.

primary-endpoint
The primary endpoint on which the SCSI target devices are visible. By default, or if you specify `all`, SCSI target devices are visible on all ports. Specify `none` if the devices should not be visible on any ports.

secondary-endpoint
The secondary endpoint on which the SCSI target devices are visible. By default, the devices are visible on all ports. The secondary port list supports path redundancy.

service-name
A SCSI target service: vtl, ddboost, or vdisk.

scsitarget initiator

`scsitarget initiator add` *`initiator-name`* `system-address` *`system-address`*
Add an initiator with the specified system address. An initiator may be added before it is visible on a transport, which allows for early provisioning.

Role required: admin.

`scsitarget initiator del` *`initiator-spec`*
Delete an initiator. Note that if the initiator is remains visible it may be automatically rediscovered.

Role required: admin.

`scsitarget initiator modify` *`initiator-spec`* `[address-method {auto | vsa | default}]`
Modify one or more initiators.

Role required: admin.

`scsitarget initiator rename` *`src-initiator-name dst-initiator-name`*
Rename an initiator.

Role required: admin.

`scsitarget initiator show detailed [`*`initiator-spec`*`] [endpoint` *`endpoint-spec`*`] [group` *`group-spec`*`]`
Show detailed information for one or more initiators, based on selected arguments.

Role required: admin, security, user, backup-operator.

`scsitarget initiator show list [`*`initiator-spec`*`] [endpoint` *`endpoint-spec`*`] [group` *`group-spec`*`]`
Display a list of initiators based on selected arguments. If no arguments are selected, the output consists of basic information for all initiator criteria.

Role required: admin, security, user, backup-operator.

Argument Definitions

auto
The device address method chosen based on the numeric LUN range being reported: 0 - 255, peripheral device addressing is used, 256 - 16383, flat device addressing is used (default).

endpoint-spec
A list of endpoints (logical names for target ports on a Data Domain system) that uses a wildcard.

group-spec
A list of access groups that uses a wildcard. This can be a vdisk *group-spec*.

initiator-name
Name of SCSI target host initiator.

initiator-spec
A list of initiators that uses a wildcard.

system-address
The related system address of a SCSI target endpoint.

vsa
Volume set addressing (VSA). This method is used primarily for addressing virtual buses, targets, and LUNs. The HP-UX operating system selects the volume set addressing method based on inquiry data and LUN information returned by the SCSI-3 REPORT LUNS command.

scsitarget persistent-reservation

`scsitarget persistent-reservation clear [device device-spec] [initiator initiator-name]`
Clear SCSI persistent reservations.

Role required: admin.

Example 106

To clear all persistent reservations set by an initiator no longer visible to the system, enter:

```
# scsitarget persistent-reservation clear initiator ibm-initiator-17
```

`scsitarget persistent-reservation disable [service service-name]`
Disable SCSI persistent reservations.

Role required: admin.

`scsitarget persistent-reservation enable [service service-name]`
Enable SCSI persistent reservations.

Role required: admin.

`scsitarget persistent-reservation show detailed [device device-spec] [initiator initiator-name]`
Show detailed information for SCSI persistent reservations, including vdisk service. Be aware that if a device does not include a reservation key, or is using a shared key, a series of zeros (0X0000000000000000) will be displayed in the Reservation Key category, instead of n/a, which is the expected behavior.

Role required: admin, security, user, backup-operator, none.

`scsitarget persistent-reservation show list [device device-spec] [initiator initiator-name]`
Show summary information for SCSI persistent reservations, including vdisk service.

Role required: admin, security, user, backup-operator, none.

Argument Definitions

device-spec
A list of devices that uses wildcards. This can be a vdisk *device-spec*.

initiator-name
Name of SCSI target host initiator.

service-name
A SCSI target service: vtl, ddboost, or vdisk.

scsitarget reset

`scsitarget reset detailed-stats`
Reset detailed statistics for a SCSI target subsystem.

Role required: admin, security, user, backup-operator, none.

scsitarget service

`scsitarget service refresh [service]`
Refresh SCSI target service configuration. All services, including vdisk, within the SCSI target system configuration will be re-created.

Role required: admin.

`scsitarget service show list`
Display a list of configured services, including vdisk, and current state.

Role required: admin, security, user, backup-operator, none.

```
# scsitarget service show list
SCSI Target Services
Service       Status
-----------   -----------------
VTL           Running
DD-Boost FC   Shutdown/Inactive
VDISK         Running
-----------   -----------------
```

scsitarget show

`scsitarget show config`
Show SCSI target configuration.

Role required: admin, security, user, backup-operator, none.

`scsitarget show detailed-stats`
Show detailed statistics for the SCSI target subsystem.

Role required: admin, security, user, backup-operator, none.

scsitarget status

`scsitarget status`
Show SCSI target status.

- The `administrative` state shows the overall state of the SCSI target subsystem.
- The `process` state shows if the SCSI target management process is currently running.
- The `module` state shows if required system modules have been loaded prior to starting the management process.

If the status shows an administrative state of `enabled` but a process state of `stopped`, you can use `scsitarget enable` to request a start of the SCSI target subsystem.

Role required: admin, security, user, backup-operator, none.

scsitarget trace

`scsitarget trace disable [component {all | user | kernel | default | component-list}]`
Disable SCSI target tracing.

Role required: admin.

`scsitarget trace enable [component {all | user | kernel | default | component-list}] [level {all | high | medium | low}] [timeout {never | timeout-mins}] [service service-name]`
Enable SCSI target tracing. If no components are specified, the default components are used. If no timeout is given, a 10-minute timeout is used. Use `scsitarget trace show` to see which components are available for each type (all, default, user, kernel).

Role required: admin.

`scsitarget trace show [component {all | user | kernel | default | component-list}]`
Show SCSI target trace status, which includes vdisk service.

Role required: admin, security, user, backup-operator, none.

```
# scsitarget trace show
Component Name  Level   Timeout (min)  Service
--------------  ------  -------------  -------
service         medium          9 mins    VDISK
```

Argument Definitions

all
Show all information about the object specified by the command option.

component
Components available for tracing: all, default, user, kernel.

component-list
List of tracing components. One or more may be specified.

`vhba`

`scst`

`fc`

`ddcl`

`vtc`

`vmc`

`vtlprocess`

`group`

`vscsi`

`vtlsm`

`vtc_readahead`

`info_cache`

`persistent_reservations`

`master_client`

`master_server`

`worker_client`

`worker_server`

`vdev_thread`

`registry`

`misc`

Note

Components `master_client`, `master_server`, `worker_client`, and `worker_server` are used only for GDA, which is no longer supported as of 5.4.

---

level
Degree of debugging verbosity to enable (`all` | `high` | `medium` | `low` | `none`).

service-name
A SCSI target service: vtl, ddboost, or vdisk.

timeout
Set how long debugging is enabled for the specified components.

scsitarget transport

`scsitarget transport option reset {`*`option-name`* | `all}`
Reset a SCSI target transport option.

Role required: admin.

`scsitarget transport option set` *`option-name value`*

Set a SCSI target transport option.

Role required: admin.

`scsitarget transport option show {`*`option-name`*` | all}`
Show a SCSI target transport option.

Role required: admin, security, user, backup-operator, none.

Example 107

```
# scsitarget transport option show loop-id transport fc
```

`scsitarget transport show stats`
Show SCSI target transport statistics.

Role required: admin, security, user, backup-operator, none.

Argument Definitions

option-name
The specific SCSI target transport option, which can be loop-id or wwnn-scope.

value
The value for the specific option.

CHAPTER 28

smt

The `smt` command manages the EMC Data Domain Secure Multi-Tenancy (SMT) software option. See the *EMC Data Domain Operating System Administration Guide* for instructions on how to create and administer multiple tenant-units on a single Data Domain system.

This chapter contains the following topics:

smt Change History

This section provides a list of changes since the 5.4 release, for all 5.5.x releases, in order of the most recent release to the first release.

New Commands in DD OS 5.5
The smt commands are a new feature in the DD OS 5.5 release.

smt Guidelines and Restrictions

- The Secure Multi-Tenancy (SMT) software option is available on DD OS versions 5.5 and later.
- Details on SMT are documented in the *EMC Data Domain Operating System Administration Guide.*

smt disable

`smt disable`
Disable the SMT software option. Disabling SMT requires unassigning tenant-unit MTrees prior to running the command `smt disable`. When an MTree is unassigned from a tenant-unit, the MTree remains on the Data Domain system and functionality is unaffected. See the *EMC Data Domain Operating System Administration Guide* for more information.

Role required: admin.

smt enable

`smt enable`
Enable the SMT software option.

Required role: admin

smt status

`smt status`
View the status of the SMT software option. SMT is either enabled or disabled.

Required role: admin.

smt tenant-unit

`smt tenant-unit create` *`tenant-unit`*
Create a tenant-unit. Tenant-units are initially created using the SMT configuration wizard. See the *EMC Data Domain Operating System Administration Guide* for details.

Role required: admin.

`smt tenant-unit destroy` *`tenant-unit`*
Destroy a tenant-unit. Tenant-units must be destroyed before the SMT software option can be disabled.

Role required: admin.

`smt tenant-unit management-group assign` *`group`* `tenant-unit` *`tenant-unit`* `[role {tenant-admin | tenant-user}]`
Assign an AD or NIS management group to a tenant-unit in the role of tenant-admin or tenant-user. See the *EMC Data Domain Operating System Administration Guide* for details.

Role required: admin.

`smt tenant-unit management-group show [`*`tenant-unit`*` | all]`
Show the management group assigned to one or all tenant-units.

Role required: admin.

`smt tenant-unit management-group unassign` *`group`* `tenant-unit` *`tenant-unit`*
Unassign an AD or NIS management group from a tenant-unit.

Role required: admin.

`smt tenant-unit management-user assign` *`user`* `tenant-unit` *`tenant-unit`* `[role {tenant-admin | tenant-user}]`
Assign a user from a management group to a tenant-unit in the role of tenant-admin or tenant-user. See the *EMC Data Domain Operating System Administration Guide* for details.

Role required: admin.

`smt tenant-unit management-user show [`*`tenant-unit`*` | all]`
Show user access information for a specific-tenant unit or for all tenant-units.

Role required: admin.

`smt tenant-unit management-user unassign` *`user`* `tenant-unit` *`tenant-unit`*
Unassign a management group user from a tenant-unit.

Role required: admin.

`smt tenant-unit option reset` *`tenant-unit`* `{self-service}`
Reset the tenant self-service option for the specified tenant unit.

Role required: admin.

`smt tenant-unit option set` *`tenant-unit`* `self-service {enabled | disabled}`
Enable or disable the tenant self-service option for the specified tenant-unit.

Role required: admin.

`smt tenant-unit option show {`*`tenant-unit`*` | all}`
Show options for a specified tenant-unit or for all tenant-units.

Role required: admin.

`smt tenant-unit rename` *`tenant-unit new-name`*
Rename a tenant-unit.

Role required: admin.

`smt tenant-unit setup` *`tenant-unit`*
Enter tenant-unit values as prompted by the SMT configuration wizard.

Role required: admin.

`smt tenant-unit show detailed [`*`tenant-unit`*` | all]`
Show detailed information for specific tenant-units or for all tenant-units.

Role required: admin.

`smt tenant-unit show list [`*`tenant-unit`*` | all]`
Show list of all tenant units or for a specific tenant-unit.

Role required: admin.

CHAPTER 29

snapshot

The `snapshot` command manages MTrees snapshots. MTrees add granularity to filesystem-type operations, allowing operations to be performed on a specific MTree instead of the entire filesystem. Snapshots are useful for avoiding version skew when backing up volatile data sets, such as tables in a busy database, and for restoring previous versions of a deleted directory or file.

A snapshot is a read-only copy of the Data Domain MTree from the top of each MTree: `/data/col1/`*mtree-name*.The MTree `/data/col1/backup` is the default directory created in the system during installation. It is also the MTree that is refreshed during an upgrade procedure. The directory `/backup` points to the default MTree. Snapshots can be accessed from the directories `/backup/.snapshot` or `/data/col1/`*mtree-name*`/.snapshot`.

This chapter contains the following topics:

snapshot Change History

This section provides a list of changes since the 5.4 release, for all 5.5.x releases, in order of the most recent release to the first release.

Modified Arguments in DD OS 5.5

snapshot list mtree

Modified to use `tenant-unit`.

Modified Output in DD OS 5.5

snapshot list mtree

Modified to display `tenant-unit`.

snapshot Guidelines and Restrictions

- If the Data Domain system is a source for collection replication, snapshots are replicated.
- If the Data Domain system is a source for directory replication, snapshots are not replicated. Snapshots must be created separately on a directory replication destination.
- Snapshots are replicated for MTrees.
- The .snapshot directory is a virtual directory. It can be referenced in any directory, but it does not show up as a directory listing except at export points (for example, a CIFS share or NFS mount point).
- The maximum number of snapshots allowed to be stored on a system is 750. If the maximum number is reached, the system generates an alert. You can resolve this by expiring snapshots and then running the command option filesys clean.
- When creating a snapshot schedule, the retention period must be set in days only. If set in hours an error message appears stating your data is in danger and the command will fail.

snapshot create

`snapshot create` *`snapshot`* `mtree` *`mtree-path`* `[retention {`*`date`* `|` *`period`*`}]`

Create a snapshot. Naming conventions for creating MTrees include uppercase and lowercase letters A-Z, a-z), numbers 0-9, single, non-leading embedded space, exclamation point (!), hash (#), dollar sign ($), ampersand (&), caret (^), tilde (~), left and right parentheses ((or)), left and right brackets ([or]), left and right curly braces ({ or }). Role required: admin, backup.

Argument Definitions

snapshot

A name for the snapshot.

mtree ***mtree-path***

The pathname of the MTree for which the snapshot is being created. The base of the path must be `/data/col1/`*`mtree_name`* or `/backup`.

retention *date*
A four-digit year, two-digit month, and two-digit day separated by dots, slashes, or hyphens. For example, 2013.03.23. The snapshot is retained until midnight (00:00, the first minute of the day) of the designated date.

retention *period*
Number of days, weeks (wks), or months (mos) to retain a snapshot. Note there is no space between the number and time period; for example, 4wks. Also, one month equals 30 days. The snapshot is retained until the same time of day it was created.

Example 108

If a snapshot was created at 8:48 a.m. on March 1, 2013 with a retention period of one month, it would be retained for 30 days.

```
# snapshot create test22 mtree /backup retention 1mos
```

snapshot expire

`snapshot expire` *`snapshot`* `mtree` *`mtree-path`* `[retention {`*`date`* `|` *`period`* `| forever}]`
Set or reset the retention time of a snapshot. To expire a snapshot immediately, use the `snapshot expire` operation with no options. An expired snapshot remains available until the next `filesystem clean` operation. Role required: admin.

Argument Definitions

snapshot
The name of the snapshot.

mtree *mtree-path*
The pathname of the MTree for which the snapshot is being created.

retention *date*
A four-digit year, two-digit month, and two-digit day separated by dots (.), slashes (/), or hyphens (-). With a retention *date*, the snapshot is retained until midnight (00:00, the first minute of the day) of the designated date.

retention *period*
Number of days, weeks (wks), or months (mos) to retain snapshot. Note there is no space between the number and time period; for example, 4wks. Also, one month equals 30 days. The snapshot is retained until the same time of day it was created. The retention period must be set in days only.

retention *forever*
The snapshot does not expire.

snapshot list

`snapshot list mtree` *`mtree-path`* `| tenant-unit` *`tenant-unit`*
View a list of snapshots of a specific MTree. The display shows the snapshot name, the amount of pre-compression data, the creation date, the retention date, and the status. The status may be blank or expired. Role required: admin, user, backup-operator, tenant-admin, tenant-user, security, none.

Example 109 Argument Definitions

tenant-unit
A tenant unit is a secure, isolated partition for tenant-specific data and control flow within a Data Domain system.

```
# snapshot list mtree /data/col1/ddmtree1
```

snapshot rename

`snapshot rename snapshotnew-name mtree mtree-path`
Rename a snapshot for a specific MTree. Role required: admin.

Example 110

To change the name from snap1 to new-snap1 for an MTree named /newMTree, enter:

```
# snapshot rename snap1 new-snap1 mtree /backup
```

snapshot schedule

`snapshot schedule add name mtrees mtree-list`
Add multiple MTrees to a single snapshot schedule. Role required: admin.

`snapshot schedule create name [mtrees mtree-list] [days days] time time [,time ...] [retention period] [snap-name-pattern pattern]`

`snapshot schedule create name [mtrees mtree-list] [days days] time time every mins [retention period] [snap-name-pattern pattern]`

`snapshot schedule create name [mtrees mtree-list] [days days] time time-time [every <hrs | mins>] [retention period] [snap-name-pattern pattern]`
Use these commands to create a snapshot schedule for multiple MTrees. Command arguments determine the duration of the schedule. (Note the different arguments for specifying time interval.) Role required: admin.

⚠ CAUTION

The retention period must be set in days only. If set in hours an error message appears stating your data is in danger and the command will fail.

Example 111

In the following example, snapshots are spaced one minute apart.

```
# snapshot schedule create sm1 mtrees /data/col1/m1 time
00:00-23:00 every 1mins retention 1days
```

`snapshot schedule del` *name* `mtrees` *mtree-list*
Remove a list of MTrees from a schedule. Role required: admin.

`snapshot schedule destroy [`*name* `| all]`
Remove the name of a schedule. Role required: admin.

`snapshot schedule modify` *name* `[mtrees` *mtree-list*`] [days` *days*`] time` *time* `[,`*time* `...] [retention` *period*`] [snap-name-pattern` *pattern*`]`

`snapshot schedule modify` *name* `[mtrees` *mtree-list*`] [days` *days*`] time` *time* `every` *mins* `[retention` *period*`] [snap-name-pattern` *pattern*`]`

`snapshot schedule modify` *name* `[mtrees` *mtree-list*`] [days` *days*`] time` *time-time* `every` *hrs* `|` *mins*`] [retention` *period*`] [snap-name-pattern` *pattern*`]`
Use these commands to modify a snapshot schedule. Command arguments determine the duration of the schedule. (Note the different arguments for specifying time interval.) Role required: admin.

`snapshot schedule reset`
Reset a snapshot schedule and delete all snapshot schedules. Role required: admin.

⚠ CAUTION

This command deletes the previous schedule without prompting the user.

`snapshot schedule show [`*name* `| mtrees` *mtree-list* `| [tenant-unit` *tenant-unit*`]]`
Show a specific schedule and show schedules associated with a specific MTree. To show a list of schedules, enter the command with no options. Role required: admin, user, backup-operator, tenant-admin, tenant-user, security, none.

Argument Definitions

tenant-unit (Optional)
The basic unit of a multi-tenancy configuration. A tenant unit is a secure, isolated partition for tenant-specific data and control flow within a Data Domain system.

snapshot Additional Topics

This section provides additional information on various topics and concepts.

Naming Snapshots Created by a Schedule

The naming convention for scheduled snapshots is the word `scheduled` followed by a four-digit year, a two-digit month, a two-digit day, a two-digit hour, and a two-digit minute. All elements of the name are separated by hyphens. For example, `scheduled-2013-04-28-13-41`.

The name `every_day_8_7` is the name of a snapshot schedule. Snapshots generated by that schedule might have the names `scheduled-2013-03-25-20-00`, `scheduled-2013-03-26-20-00`, and so forth.

Example 112

Example 112 (continued)

To schedule a snapshot every Monday and Thursday at 2:00 a.m. with a retention of two months, enter:

```
# snapshot create schedule mon thu 02:00 retention 2mos
```

CHAPTER 30

snmp

The `snmp` command enables or disables SNMP access to a Data Domain system, adds community strings, gives contact and location information, and displays configuration settings.

SNMP management requires two primary elements: an SNMP manager and an SNMP agent. An SNMP *manager* is software running on a workstation from which an administrator monitors and controls the different hardware and software systems on a network. These devices include, but are not limited to, storage systems, routers, and switches.

An SNMP *agent* is software running on equipment that implements the SNMP protocol. SNMP defines how an SNMP manager communicates with an SNMP agent. For example, SNMP defines the format of requests that an SNMP manager sends to an agent and the format of replies the agent returns.

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 enables administrative users to configure community strings, hosts, and other SNMP MIB variables on the Data Domain system.

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.

This chapter contains the following topics:

snmp Change History

This section provides a list of changes since the 5.4 release, for all 5.5.x releases, in order of most recent release to first release.

New Commands in DD OS 5.5

snmp set sysNotes *sysNotes*
Set the SNMP system notes MIB variable to record system-specific data not stored in other SNMP variables.

snmp show stats
Show the SNMP operating statistics.

snmp show sysNotes
Show the SNMP system notes MIB variable.

Modified Output in DD OS 5.5

snmp show config [version {v2c | v3}]
The output now displays the system notes variable configuration.

snmp Guidelines and Restrictions

- Data Domain systems support MIB access from management stations using SNMPv1, v2C, and v3.
- Data Domain system can send traps using SNMP v2c or SNMP v3.
- Default port 161 is used for inbound/outbound, read/write SNMP access. Default port 162 is used for outbound traffic for SNMP traps.
- Spaces, tabs, colons, semicolons, U.S. dollar signs, and quotation marks cannot be used in community strings.
- To change multiple settings quickly and avoid restarting SNMP, run the `snmp disable` command, change the settings, and then run `snmp enable`.

snmp add

`snmp add ro-community` *`community-string-list`* `[hosts` *`host-list`*`]`
Add one or more community strings for read-only access to the Data Domain system. A common string for read-only access is public. To grant access to specific hosts, enter the names in *host-list*. Role required: admin.

Example 113

A valid host list can include both hostnames and IP addresses.

```
hostnameA,hostNameB 10.10.1.2,10.10.1.310.**
```

Example 114

The following command adds a community string of public with read-only permissions.

Example 114 (continued)

```
# snmp add ro-community public hosts host.emc.com
```

`snmp add rw-community` *community-string-list* `[hosts` *host-list*`]`
Add one or more community strings for read/write access to the Data Domain system. A common string for read/write access is private. To grant access to specific hosts, enter the names in *host-list*. Role required: admin.

Example 115

The following command adds a community string of private with read/write permissions.

```
# snmp add rw-community private hosts host.emc.com
```

`snmp add trap-host` *host-name-list*`[:port] [version {v2c | v3}] [{community` *community* `| user` *user*`}]`
Add one or more trap hosts (host name or IP address) to receive the SNMP traps generated by the Data Domain system. Note that alerts are also sent as traps, even when the local SNMP agent is disabled. By default, port 162 is used to send traps, but another port may be assigned.

SNMP trap-host supports SNMPv2c and v3. For SNMPv1 and v2c specify the version and the pre-existing community. For SNMPv3 specify the SNMPv3 user name. Make sure to include trap-host in the community string hosts. Role required: admin.

Example 116

The following command adds trap host admin12.

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

snmp del

`snmp del ro-community` *community-string-list* `[hosts` *host-list*`]`
Delete one or more community strings for read-only access to the Data Domain system. Role required: admin.

`snmp del rw-community` *community-string-list* `[hosts` *host-list*`]`
Delete one or more community strings for read-write access to the Data Domain system. Role required: admin.

Example 117

The following command deletes the community string private with read/write permissions.

```
# snmp del rw-community private hosts myhost.emc.com
```

Example 118

Example 118 (continued)

The following command deletes the community private and all hosts associated with private.

```
# snmp del rw-community private
```

`snmp del trap-host` *host-name-list*
Delete one or more trap hosts from the list of hosts receiving SNMP traps generated by the Data Domain system. Role required: admin.

Example 119

The following command deletes trap host admin12.

```
# snmp del trap-host admin12
```

snmp disable

`snmp disable`
Disable SNMP and close port 161. Role required: admin.

snmp enable

`snmp enable`
Enable SNMP and open port 161. Role required: admin.

snmp reset

`snmp reset`
Reset SNMP agent configuration to default values. Role required: admin.

`snmp reset ro-communities`
Reset list of read-only community strings to default values. Role required: admin.

`snmp reset rw-communities`
Reset list of read-write community strings to default values. Role required: admin.

`snmp reset sysContact`
Reset the SNMP administrative contact MIB variable to the default value or to an empty string if the system value is empty. Role required: admin.

`snmp reset sysLocation`
Reset the system location MIB variable to the default value or to an empty string if the system value is empty or to an empty string if the system value is empty. Role required: admin.

`snmp reset trap-hosts`
Reset list of SNMP trap receiver hosts to default values. Role required: admin.

snmp set

`snmp set sysContact` *sysContact*

Set the SNMP administrative contact MIB variable. The SNMP sysContact MIB variable differs from the value set with the `config set admin-email` command option. However, if the SNMP MIB variables are not set with the SNMP commands, the variables default to the system values given with the `config set` commands. Role required: admin.

`snmp set sysLocation` *`sysLocation`*
Set the SNMP physical location MIB variable. The SNMP sysLocation MIB variables differs from the value set with the `config set location` command option. However, if the SNMP MIB variables are not set with the SNMP commands, the variables default to the system values given with the `config set` commands. Role required: admin.

`snmp set sysNotes` *`sysNotes`*
Set the SNMP system notes MIB variable to record system-specific data not stored in other SNMP variables. Role required: admin.

snmp show

`snmp show config [version {v2c | v3}]`
Use this command to display all SNMP parameters. If SNMP `version` is not entered, output displays information for both versions. Role required: admin, security, user, backup-operator, or none.

`snmp show ro-communities`
Show the SNMP read-only community strings. Role required: admin.

`snmp show rw-communities`
Show the SNMP read/write community strings. Role required: admin.

`snmp show stats`
Show the SNMP operating statistics. Role required: admin, security, user, backup-operator, or none.

`snmp show sysContact`
Show the SNMP administrative contact MIB variable. Role required: admin, security, user, backup-operator, or none.

`snmp show sysLocation`
Show the SNMP physical location MIB variable. Role required: admin, security, user, backup-operator, or none.

`snmp show sysNotes`
Show the SNMP system notes MIB variable. Role required: admin, security, user, backup-operator, or none.

`snmp show trap-hosts [version {v2c | v3}]`
Display the trap host list on a Data Domain system. If SNMP `version` is not entered, output displays information for both versions. Role required: admin, security, user, backup-operator, or none.

snmp status

`snmp status`
Show SNMP status. Role required: admin, security, user, backup-operator, or none.

snmp user

`snmp user add` *user-name* `access {read-only | read-write} [authentication-protocol {MD5 | SHA1} authentication-key` *auth-key* `[privacy-protocol {AES | DES} privacy-key` *priv-key*`]]`

Add an SNMPv3 user to the system specifying the access rights, authentication protocol, and privacy protocol. The authentication key is used when calculating the digest for the authentication protocol. The privacy key is used as input for the privacy protocol. Role required: admin.

`snmp user del` *user-name*

Delete an SNMPv3 user. Role required: admin.

`snmp user modify` *user-name* `access {read-only | read-write} [authentication-protocol {MD5 | SHA1} authentication-key` *auth-key* `[privacy-protocol {AES | DES} privacy-key` *priv-key*`]]`

Modify an SNMPv3 user settings such as access rights, authentication protocol, and privacy key. Role required: admin.

`snmp user reset`

Reset list of SNMPv3 users to default values. Role required: admin.

`snmp user show` *user-name*

Display a SNMPv3 user. Role required: admin, security, user, backup-operator, or none.

CHAPTER 31

storage

The `storage` command adds, removes, and displays disks and LUNs belonging to active and archive storage tiers. Tiered storage enables the Data Domain system to use different types of storage devices.

A storage tier can contain two types of storage: whole disks in an enclosure, such as a Data Domain system or attached expansion shelf, or LUNs in a Data Domain gateway system that uses a SAN.

System storage for a filesystem or associated RAID disk group consists of two storage tiers: one active and one archive. The active tier has one active unit of storage, and the archive tier has one or more retention units of storage.

This chapter contains the following topics:

storage Change History

There have been no changes to this command since the 5.4.x release.

storage Guidelines and Restrictions

- After adding disks or LUNs to storage tiers, the storage must be provisioned by creating or expanding the filesystem.
- Available LUNs may be removed from a tier to use as a RAID hot spare.

storage add

`storage add [tier {active | archive}] {enclosure` *`enclosure-id`* `| dev`*`disk-id`* `[spindle-group` *`1-16`*`] | disk` *`enclosure-id.disk-id`* `}`
Add storage devices to a tier. Device types include all disks in an enclosure, a single disk, or a LUN in a gateway system. Disks or LUNs must be in the `Unknown` state to be added to the designated tier, after which the state changes to Available. This command cannot be used on dataless head (DLH) units. Default spindle group is 1.

Additionally:

- If adding a disk to an enclosure on the active tier and if there is already a disk group in the enclosure, the disk becomes a spare, not available. This is because if you add a disk and it becomes available, there is no way for the available disk to become spare. Spares are only created when a disk group is created within the enclosure. This rule also applies to the head unit.
- If there is not a disk group in the enclosure (other disks are available or spare), the disk becomes available.

Note

The `storage add dev`*`disk-id`* command option is allowed only after running the command option `storage add enclosure` *`enclosure-id`* to add the shelf.

Role required: admin.

Example 120

To add disks in two different enclosures to the active tier:

```
# storage add enclosure 2
# storage add enclosure 5
```

storage remove

`storage remove {enclosure` *`enclosure-id`* `| dev`*`disk-id`* `| disk` *`enclosure_id.disk-id`*`}`
Remove storage devices from the tier, including all disks in an enclosure, a single disk, or a LUN in a gateway system. You can also remove a disk from a DLH unit. When a device is removed the state changes to `Unknown`.

This command cannot remove an In Use disk if doing so exceeds the minimum number allowed by the RAID scheme. This command also cannot remove a disk if the disk is a spare or an `In Use` LUN. Role required: admin.

storage show

`storage show {all | summary | tier {active | archive}}`

Display information about filesystem storage. All users may run this command option.

Output includes the number of disk groups working normally and the number of degraded disk groups. Details on disk groups undergoing, or queued for, reconstruction, are also shown when applicable. The abbreviation N/A in the column Shelf Capacity License Needed indicates the enclosure does not require a capacity license, or that part of the enclosure is within a tier and the capacity license for the entire enclosure has been accounted for. Role required: admin, security, user, backup-operator, or none.

Disk States

absent
No disk is in the disk slot.

available
Any of the following:

- A previously unknown disk or LUN added to a tier by the `storage add enclosure` command option.
- DD Extended Retention system only: a previously `In Use` disk or LUN deleted from a retention unit by the `filesys archive unit del` command option. This operation reverts the disk or LUN to available storage in the archive tier.
- A previously failed disk in an expansion shelf populated with other disks belonging to a tier that is not primarily composed of disk group disks, and whose partition was destroyed by the `disk unfail` command.

Failed
Tiered storage (`Available`, `Spare`, or `In Use`) removed from the tier automatically by the disk subsystem, or explicitly by an administrative user. Failed may also indicate unknown or foreign storage explicitly changed to the `Failed` state.

Foreign
A disk belonging to a third-party vendor.

In Use
Storage that is part of an active filesystem or associated RAID disk group.

Spare
A disk that can be used as a RAID hot spare through RAID reconstruction. Spare disks can be used to create or expand the filesystem.

Spare (reconstruction)
A spare disk that is pending or undergoing RAID reconstruction, which puts filesystem data into what the formerly spare disk and then makes the disk an integral part of a disk group. After RAID reconstruction of a spare disk completes, the disk is part of a RAID disk group.

unknown
A blank disk inserted into the disk slot, or a disk failed by a RAID system.

CHAPTER 32

support

The `support` command manages bundles (EMC Data Domain log files), traces (performance log files, also known as `perf.logs`), and file lists (file names under `/ddvar`) from a customer Data Domain system. The information is transported to EMC via HTTP or HTTPS.

This chapter contains the following topics:

support Change History

This section provides a list of changes since the 5.4 release, for all 5.5.x releases, in order of most recent release to first release.

New Commands in DD OS 5.5

support coredump delete {*core-file-list* | all}
Delete the specified coredump files or delete all coredump files. File names in a list must be separated by a space or a comma.

support coredump list
List the coredump files on the system.

support bundle delete {*bundle-name-list* | all}
Delete some or all of the support bundles on the system. File names in a list must be separated by a space or a comma.

support bundle resume *bundle-name* [transport {http | https}]
If a support bundle upload fails before completion, use this command to resume the upload from where it left off (instead of starting from the beginning).

Modified Output in DD OS 5.5

support bundle list
List support bundle files using the new name format, which is described in the *EMC Data Domain Operating System Administration Guide*.

support bundle create {files-only *file-list* | traces-only} [and-upload [transport {http | https}]]
The following line is added to the output: `Generating Autosupport Report...` Also, a prompt appears if you attempt to create more than 10 support bundles.

support bundle create default [with-files *file-list*] [and-upload [transport {http | https}]]
The following line is added to the output: `Generating Autosupport Report...` Also, a prompt appears if you attempt to create more than 10 support bundles.

support bundle

`support bundle create {files-only` *`file-list`* `| traces-only} [and-upload [transport {http|https}]]`
Compress listed files into bundle and upload if specified. File names in a list must be separated by a space or a comma. You are prompted to delete an older bundle and continue if 10 support bundles exist on the system. Role required: admin.

`support bundle create default [with-files` *`file-list`*`] [and-upload [transport {http|https}]]`
Compress default and listed files into bundle and upload if specified. File names in a list must be separated by a space or a comma. You are prompted to delete an older bundle and continue if 10 support bundles exist on the system. Role required: admin.

Example 121

Example 121 (continued)

```
# support bundle create default and-upload

Reached maximum limit of bundles. To create a new bundle,
old bundle "ash-ddr-traces-130402194020.tar.gz" will be
deleted.
Do you want to continue? (yes|no) [yes]:
```

`support bundle delete {`*`bundle-name-list`* `| all}`
Delete some or all of the support bundles on the system. File names in a list must be separated by a space or a comma. Role required: admin.

`support bundle list`
List all support bundles on system. Role required: admin.

`support bundle resume` *`bundle-name`* `[transport {http|https}]`
If a support bundle upload fails before completion, use this command to resume the upload from where it left off (instead of starting from the beginning). Role required: admin.

`support bundle upload` *`bundle-name`* `[transport {http | https}]`
Upload specified bundle to support server. Role required: admin.

support coredump

`support coredump delete {`*`core-file-list`* `| all}`
Delete the specified coredump files or delete all coredump files. File names in a list must be separated by a space or a comma. Role required: admin.

`support coredump list`
List the coredump files on the system. Role required: admin.

support notification

`support notification disable {autosupport | alerts | all}`
Disable email notification to EMC Data Domain for the specified option. Disabling autosupport disables the daily autosupport email. Disabling alerts disables all alert email, including both current alerts and summary reports. The all option specifies that reporting of both autosupport and alerts is to be disabled. Role required: admin.

`support notification enable {autosupport | alerts | all}`
Enable email notification to EMC Data Domain for the specified option. Enabling autosupport enables the daily autosupport email. Enabling alerts enables all alert email, including both current alerts and summary reports. The all option specifies that reporting of both autosupport and alerts is to be enabled. Role required: admin.

`support notification show {autosupport | alerts | all}`
Show the notification configuration for the autosupport and alerts options. Role required: admin, security, user, backup-operator, or none.

CHAPTER 33

system

The `system` command enables administrative users to perform standard tasks on Data Domain systems, configure a system for Retention Lock Compliance, and view system-level information.

This chapter contains the following topics:

system Change History

This section provides a list of changes since the 5.4 release, for all 5.5.x releases, in order of most recent release to first release.

New Commands in DD OS 5.5.2

system passphrase option reset min-length
Reset the system passphrase min-length option to the default value.

system passphrase option set min-length *length*
Set the minimum length for the system passphrase.

system passphrase option show [min-length]
Show the system passphrase minimum length configuration.

Modified Output in DD OS 5.5.2

system show performance [local] [raw | fsop | view {legacy | default} custom-view {state | throughput | protocol | compression | streams |utilization | mtree-active},...] [duration *duration* {hr | min} [interval *interval* {hr | min}]]
Added two columns to the Streams section for replication in and replication out streams.

Modified Output in DD OS 5.5.1

system show all
For newer systems, this command now displays the product serial number as the serial number instead of the chassis serial number. The chassis serial number is also displayed.

system show serialno [detailed]
For newer systems, this command now displays the product serial number as the serial number instead of the chassis serial number. The `detailed` argument displays both the system serial number and the chassis serial number.

New Commands in DD OS 5.5

system add-on
The `system add-on` commands are part of future enhancements to DD OS. The use of these commands and any related content associated with these commands will only come directly from EMC Data Domain Support or Engineering. Any other use or attempted use of these commands could adversely affect the stability of your Data Domain system.

system add-on install *file*

system add-on list

system add-on show history [all]

system add-on uninstall *add-on*

system add-on upgrade *file*

system package del *file*
Deletes the specified package file.

system package list *file*

If the file attribute is omitted, this command lists all files in the `/ddvar/releases` directory, which is where package files are stored. If the file attribute is specified, this command lists information about the specified package file.

Modified Arguments in DD OS 5.5

system show performance [local] [raw | fsop] [*duration* {hr | min} [*interval* {hr | min}]]

Additional arguments allow you to create custom performance views.

`system show performance [local] [raw | fsop | view {legacy | default} custom-view {state | throughput | protocol | compression | streams |utilization | mtree-active},...] [duration *duration* {hr | min} [interval *interval* {hr | min}]]`

system show stats [view {nfs | cifs | repl | net | iostat | sysstat},...] [custom-view *view-spec*,...] [{local | gda-display {row | column}}] [interval *nsecs*] [count *count*]

This command now has an option for DD Boost statistics.

`system show stats [view {nfs|cifs|repl|net|iostat|sysstat|ddboost},...] [custom-view *view-spec*,...] [{local | gda-display {row | column}}] [interval *nsecs*] [count *count*]`

Modified Behavior in DD OS 5.5

system show date

This command is now available to users with tenant-admin or tenant-user roles.

system show version

This command is now available to users with tenant-admin or tenant-user roles

Modified Output in DD OS 5.5

system retention-lock compliance status

This command now includes accumulated clock variance (clock skew) information.

system show stats [view {nfs | cifs | repl | net | iostat | sysstat | ddboost},...] [custom-view *view-spec*,...] [{local | gda-display {row | column}}] [interval *nsecs*] [count *count*]

This command can now display DD Boost statistics.

Deleted Commands in DD OS 5.5

system package show *file*

Use this:

`system package list *file*`

.

system Guidelines and Restrictions

- The battery entry for NVRAM cards should show as 100 percent charged, enabled. Exceptions are if the system is new or the card is a replacement. In both cases the charge may be less than100 percent initially; however, if it does not reach 100 percent within three days, or if a battery is not enabled, the card must be replaced.

system headswap

`system headswap`
Restore the configuration to a system after replacing the head unit. For additional instructions, see the Chassis Replacement FRU document for the system mode and the *EMC Data Domain System Controller Upgrade Guide*. Role required: admin.

Note

After you enter this command, the system displays a message that reminds you that you will need the passphrase for the old system if encryption was enabled on that system. You must type **`yes`** to continue.

system option

`system option reset {login-banner}`
Configure no login banner (no filename specified) or set the banner to that defined in the specified file. Role required: admin.

`system option set console {serial | lan | monitor}`
Set the active console option as follows:.

- For a Serial Over LAN (SOL) connection, enter `system option set console lan`.
- For a console connection through the serial port, enter `system option set console serial`.
- For a console connection through the monitor port (which is not available on all systems), enter `system option set console monitor`.

Role required: admin.

`system option set login-banner` *`file`*
Set the login banner file. Role required: admin.

Example 122

To create a banner message for your system, mount the Data Domain system directory, `/ddvar`, from another system, create a text file with your login message in `/ddvar`, and then enter the command to use the system banner. The following command selects a file named `banner` in `/ddvar`:

```
# system option set login-banner /ddvar/banner
```

`system option show`
View the configuration for the login banner file and the active console. Role required: admin.

system package

`system package del` *`file`*
Deletes the specified package file. Role required: admin.

`system package list [`*`file`*`]`

If the file attribute is omitted, this command lists all files in the /ddvar/releases directory, which is where package files are stored. If the file attribute is specified, this command lists information about the specified package file. Role required: admin, security, user, backup-operator, or none.

system passphrase

`system passphrase change`

Change the passphrase used to access the system. You must disable the file system before using this command, and the new passphrase must contain the minimum number of characters configured with the `system passphrase option set min-length` command. Role required: admin. This command requires security officer authorization.

Example 123

The following is an example of a successful passphrase change.

```
# system passphrase change
This command requires authorization by a user having a 'security'
role.
Please present credentials for such a user below.
        Username:
        Password:
Enter current passphrase:
Enter new passphrase:
Re-enter new passphrase:
Passphrases matched.
The system passphrase has changed
```

Example 124

The passphrase change fails in the following example because the new passphrase does not conform to the configured minimum length.

```
# system passphrase change
This command requires authorization by a user having a 'security'
role.
Please present credentials for such a user below.
        Username:
        Password:
Enter current passphrase:
Enter new passphrase:
Re-enter new passphrase:
Passphrases matched.

**** New passphrase does not meet the minimum length policy.
```

`system passphrase option reset min-length`

Reset the system passphrase min-length option to the default value of 9. Role required: admin. This command requires security officer authorization.

Example 125

```
# system passphrase option reset min-length
This command requires authorization by a user having a 'security'
role.
Please present credentials for such a user below.
        Username:
        Password:
```

Example 125 (continued)

```
Passphrase option "min-length" is reset to default(9).
**   The current passphrase (length 6) must be changed to meet the new
min-length requirement.
```

`system passphrase option set min-length` *length*

Set the minimum length for the system passphrase. No minimum length is defined for new systems. The range for the minimum length is 1 to 255 characters. Role required: admin. This command requires security officer authorization.

Example 126

```
# system passphrase option set min-length 16
This command requires authorization by a user having a 'security'
role.
Please present credentials for such a user below.
        Username:
Passphrase option “min-length” set to 16.
```

Example 127

If you set a passphrase minimum length that is longer then the current passphrase length, DD OS displays a message to remind you to change the current passphrase.

```
# system passphrase option set min-length 20
This command requires authorization by a user having a 'security'
role.
Please present credentials for such a user below.
        Username:
Passphrase option “min-length” set to 20.
**   The current passphrase (length X) must be changed to meet the new
min-length requirement.
```

`system passphrase option show [min-length]`

Show the system passphrase minimum length configuration. Role required: admin.

Example 128

```
# system passphrase option show
Option       Value
----------   -----
min-length   16
----------   -----
```

`system passphrase set`

For fresh installations, set the passphrase used to access the system. The passphrase length must be longer than the configured minimum and cannot exceed 255 characters. Role required: admin.

Example 129

```
# system passphrase set
Enter new passphrase:
Re-enter new passphrase:
Passphrases matched.
The passphrase is set.
```

Example 129 (continued)

system poweroff

`system poweroff`

Shut down the Data Domain system. The command performs an orderly shutdown of filesystem processes. This command does not power off external storage. Role required: admin.

system reboot

`system reboot`

Shut down and reboot a Data Domain system. The command automatically performs an orderly shutdown of filesystem processes. Role required: admin.

system retention-lock

`system retention-lock compliance configure`

Configure Retention Lock Compliance on the Data Domain system. Role required: admin. This command option requires security officer authorization.

`system retention-lock compliance enable`

Enable Retention Lock Compliance on the Data Domain system. Role required: admin. This command option requires security officer authorization. See the command option `system retention-lock compliance configure` for instructions on configuring and enabling Retention Lock.

`system retention-lock compliance status`

Display status of the Retention Lock Compliance policy on the system, including system clock skew. Role required: admin. This command option requires security officer authorization.

system sanitize

`system sanitize abort`

Stop the system sanitization process. Role required: admin.

`system sanitize start`

Start the system sanitization process. Note that prior to running sanitization, snapshots created during a previous replication process by another user may continue to hold deleted data. To ensure data is removed from replication snapshots during system sanitization, synchronize all replication contexts prior to beginning the procedure. Role required: admin.

`system sanitize status`

Check system sanitization process status. Role required: admin.

`system sanitize watch`

Monitor the progress of system sanitization. Role required: admin.

For more information on sanitization and task-based instructions, see the *EMC Data Domain Operating System Administration Guide*.

system set

`system set date MMDDhhmm[[CC]YY]`

Set the system date and time. Do not use this command if Network Time Protocol (NTP) is enabled. This command option requires security officer authorization if the system is enabled for Retention Lock Compliance.

The data and time format uses the following elements.

- Two digits for the month, *MM* (01 through 12).
- Two digits for the day of the month, *DD* (01 through 31).
- Two digits for the hour, *hh* (00 through 23).
- Two digits for minutes, *mm* (00 through 59).
- Optional: Two digits for the century *CC* and two digits for the year *YY*.

The hour *hh* and minute *mm* variables are entered in 24-hour format with no colon between the hours and minutes. 2400 is an invalid entry. The entry 0000 equals midnight. Role required: admin.

Example 130

You can use either of the following commands (two- or four-digit year) to set the date and time to April 23, 2013, at 9:24 a.m.

```
# system set date 0423152413
# system set date 042315242013
```

system show

`system show all`

Show all system information. Note that newer systems, such as DD4500 and DD7200, display the product serial number in the Serial number row and the chassis serial number in the Chassis serial number row. On legacy systems, such as DD990 and earlier, the Serial number row displays the chassis serial number and the Service tag row displays the product serial number. The product serial number remains the same during many maintenance events, including chassis upgrades. Role required: admin, security, user, backup-operator, or none.

`system show date`

Display the system clock. Role required: admin, tenant-admin, security, user, tenant-user, backup-operator, or none.

`system show detailed-version`

Show the version number and release information. Role required: admin, security, user, backup-operator, or none.

`system show eula`

View the End User License Agreement (EULA). Note if the user is not present during system installation, the Data Domain Technical Consultant can temporarily bypass license acceptance and continue with the installation by pressing Ctrl-C. Otherwise, the user must press Enter to accept the license, which is displayed the first time he or she logs in to the system. See the *EMC Data Domain Operating System Initial Configuration Guide* for details. Role required: admin, security, user, backup-operator, or none.

`system show hardware`

Display information about slots and vendors and other hardware in a Data Domain system. Role required: admin, security, user, backup-operator, or none.

`system show managing-system`
Identify on which Data Domain Management Console the Data Domain system was added. Also display details about the Data Domain Management Console, such as the outbound proxy host and port, the date for which the system became managed, and the date of last contact. Role required: admin, security, user, backup-operator, or none.

`system show meminfo`
Display summary of system memory usage. Output differs between newer systems, such as DD4500 and DD7200, and legacy systems, such as DD990 and earlier. Role required: admin, security, user, backup-operator, or none.

`system show modelno`
Display the hardware model number of a Data Domain system. Role required: admin, security, user, backup-operator, or none.

`system show nvram`
Display information about NVRAM cards. If output indicates one or more component error, an alerts notification is sent to the designated group and the Daily Alert Summary email includes an entry citing details of problem. Role required: admin, security, user, backup-operator, or none.

`system show oemid [name | value]`
Show details of system OEM. On systems with head units and shelves, the OEM identifier of the head unit is displayed first. Output includes IDs for connected enclosures only. Role required: admin, security, user, backup-operator, or none.

`system show performance [local] [raw | fsop | view {legacy | default} custom-view {state | throughput | protocol | compression | streams |utilization | mtree-active},...] [duration` *`duration`* `{hr | min} [interval` *`interval`* `{hr | min}]]`
Display system performance statistics for a designated interval. If you enter this command without the custom-view argument, the standard performance report appears. Role required: admin, security, user, backup-operator, or none.

Argument Definitions

custom-view
Specifies a custom report that includes only those performance statistics that you specify. Valid entries specify the performance statistics to display and include the following: state, throughput, protocol, compression, streams, utilization, and mtree-active. To display multiple performance statistics, enter multiple labels in the order in which you want the statistics to appear. For example, `system show performance custom-view state streams`

duration
The hours or minutes prior to the current time for which to show data.

fsop
Display the number of each filesystem operation performed per minute.

interval
The time between each line in the display. To specify the interval, you must also specify the duration.

local
Display local statistics.

raw
Show unformatted statistics.

Example 131

To show performance figures of the prior 30-minute duration only, enter:

```
# system show performance duration 30 min
```

Example 132

To show performance figures of the prior 30-minute duration with an interval of 5 minutes between each set of figures, enter:

```
# system show performance duration 30 min interval 5 min
```

Output Definitions: Cache Miss

data
Percent of data segment lookups that miss in the cache. A high percent indicates poor data prefetching.

meta
Percent of metadata segment lookups that miss in the cache. For each data access, first perform a metadata lookup followed by a data lookup. A high percent indicates poor metadata prefetching.

ovhd
Percent of a compression unit cache block that is unused. Compression regions are stored in fixed size (128 KB) blocks. A high ovhd relative to unus indicates space is being wasted due to cache block fragmentation. In the ideal case, ovhd should exactly equal unus.

thra
Percent of compression units that have been read and discarded without being used. A high percent indicates cache thrashing.

unus
Percent of compression unit data that is unused. Because a compression unit contains multiple segments, not all segments in a compression region may be used. A high percent indicates poor data locality.

Output Definitions: Compression

gcomp
Global compression rate.

lcomp
Local compression rate.

Output Definitions: Latency

avg/sdev ms
The average and standard deviation of the response time for ddfs to service all protocol requests, excluding the time to receive or send the request or reply.

Output Definitions: SS Load Balance (user/repl)

Indicates the relative load balance across segment storage (segstore) instances. Information under (user/repl) denotes all user-plus-Replicator traffic.

prefetch avg/sdev
Prefetch requests.

stream avg/sdev
The average number of open streams and the standard deviation.

rd
The number of read requests.

rd
Read processes.

tot
The total number of requests.

SS Load Balance (gc)

Denotes type and number of expunge (gc) processes.

wr
The number of write requests.

wr
Write processes.

tot
The total number of gc processes.

Output Definitions: MTree Active

rd
The number of active read streams.

wr
The number of active write streams.

Output Definitions: Protocol

data (MB/s in/out)
Protocol throughput. Amount of data the filesystem can read from and write to the kernel socket buffer.

load
Load percentage (pending ops/total RPC ops *100).

ops/s
Operations per second.

wait (ms/MB in/out)
Time taken to send and receive 1MB of data from the filesystem to kernel socket buffer.

Note

Protocol data includes NFS, CIFS, DD Boost over IP, and DD Boost-managed replication and optimized duplication. Data does *not* include Replication, VTL over Fibre Channel, or DD Boost over Fibre Channel.

Output Definitions: State

B
GDA (Also known as multinode cluster [MNC] balancing. This functionality is no longer supported as of 5.4.)

C
Cleaning

D
Disk reconstruction

F
Archive data movement

I
Container verification (scrubbing)

M
Fingerprint merge

R
Archive space reclamation

S
Summary vector checkpoint

V
File verification running

Output Definitions: Streams

r+
The number of reopened read file streams in the past 30 seconds.

rd
The number of active read streams.

Repl in
The number of incoming replication streams.

Repl out
The number of outgoing replication streams.

w+
The number of reopened write file streams in the past 30 seconds.

wr
The number of active write streams.

Output Definitions: Throughput (MB/s)

Read
The read throughput data from the Data Domain system.

Repl Network (in/out)
Network replication throughput into and out of the Data Domain system.

Repl Pre-comp (in/out)
Replication pre-compressed (logical) throughput into and out of the Data Domain system. The value is always zero for collection replication.

Write
The write throughput data to the Data Domain system.

Note

Throughput Read and Write data includes NFS, CIFS, DD Boost over IP and Fibre Channel, VTL, Replication, DD Boost-managed replication and optimized duplication.

Output Definitions: Time Stamp

Date
The date system performance is being viewed.

Time
The time system performance is being viewed.

Output Definitions: Utilization

CPU avg/max %
The average and maximum percentage of CPU utilization.

Disk max %
The maximum percentage of disk utilization.

`system show ports`
Display information about ports. VTL-related ports do not display unless VTL is enabled. Role required: admin, security, user, backup-operator, or none.

Output Definitions

Connection Type
The type of connection, such as Ethernet, SAS, VTL, etc.

Firmware
The Data Domain system HBA firmware version.

Hardware Address
A MAC address, a WWN, or a WWPN/WWNN. An address followed by an Ethernet port number is a MAC address. WWN is the world-wide name of the Data Domain system SAS HBA on a system with expansion shelves. WWPN/WWNN is the world-wide port name or node name from the Data Domain system Fibre Channel HBA on gateway systems.

Link Speed
The speed in Gbps (Gigabits per second).

Port
The port number. See the model-specific installation and setup guide to match a slot to a port number.

`system show serialno [detailed]`
Display the system serial number. On newer systems, such as DD4500 and DD7200, the system serial number is the product serial number, which remains the same during many maintenance events, including chassis upgrades. On legacy systems, such as DD990 and earlier, the system serial number is the chassis serial number. When the `detailed` argument is specified, the output displays both the system serial number and the chassis serial number, which will be different on newer systems and identical on legacy systems. Role required: admin, security, user, backup-operator, or none.

Example 133

The following example is from a newer system that displays the product serial number as the system serial number.

```
# system show serialno detailed
Serial number: APM00132009750
Chassis Serial number: FCNME130300006
```

`system show stats [view {nfs | cifs | repl | net | iostat | sysstat | ddboost},...] [custom-view` *`view-spec`*`,...] [{local | gda-display {row | column}}] [interval` *`nsecs`*`] [count` *`count`*`]`
Display system statistics collected since the last reboot. If you enter this command without the view or custom-view arguments, the standard statistics report appears.

If the system is too busy to determine a value, the column shows a dash instead of a number. Role required: admin, security, user, backup-operator, or none.

Note

Global Deduplication Arrays are deprecated in this release. Users will receive a message if the argument gda-display is entered.

Argument Definitions

column
Displays output of for each node in column format. Column headings indicate type of stat value.

count
Specifies how many times to display the results. The default count is one. If interval is specified and count is omitted, the count is set to infinite, or until the user presses Ctrl-C.

custom-view
Specifies a custom report that includes only those statistics that you specify. Valid entries include any column section label in the standard reports: cpu, state, nfs, cifs, net (for network), disk, nvram, and repl (for replication). To display multiple column sections, enter the column labels in the order in which you want the sections to appear.

gda-display
Displays values of cluster nodes on the master system in a row or column format. Valid on the master node of a cluster only.

interval
When specifying intervals for collecting statistics, the first report is for current activity. Subsequent reports show activity performed during [`interval` *nsecs*]. The default interval is five seconds.

local
Displays local values on the master system. Valid on the master node of a cluster only.

row
Output for each node is in row format, displayed as a single line for each interval.

view
Specifies a variation of the standard statistics report that provides additional statistics for the feature specified. Valid entries are nfs for NFS, cifs for CIFS, repl for replication, net for network, iostat for IO statistics, sysstat for system statistics, and ddboost for DD Boost statistics.

Example 134

```
# system show stats view nfs interval 2
```

Output Definitions: CPU

CPU

aggr busy %
Average of busy percentage of all CPUs.

aggr max %
Amount of data sent through all interfaces.

State
Indicates system state. See the description of the show system performance command for details on what each letter represents.

CIFS

ops/s
I/O and metadata operations per second.

in MB/s
Write throughput.

out MB/s
Read throughput.

NFS

ops/s
I/O operations.

load %
Load percentage (pending ops/total RPC ops *100).x.)

data in % MB/s
Protocol throughput. Amount of data the filesystem can read from and write to the kernel socket buffer.

data out % MB/s
Protocol throughput. Amount of data the filesystem can write to the kernel socket buffer.

wait in ms/MB
Average amount of time spent in ms to receive the amount of data.

wait out ms/MB
Average amount of time spent in ms to send the amount of data.

Net

aggr in MB/s
Amount of data received through all interfaces.

aggr out MB/s
Amount of data sent through all interfaces.

`system show uptime`
Display the filesystem uptime, the time since the last reboot, the number of users, and the average load. Role required: admin, security, user, backup-operator, or none.

`system show version`
Display the Data Domain OS version and build identification number. Role required: admin, tenant-admin, security, user, tenant-user, backup-operator, or none.

system status

`system status`
Display status of fans, internal temperatures, and power supplies. Information is grouped separately for the Data Domain system and each expansion shelf connected to the system. See the *EMC Data Domain Operating System Administration Guide* for details. Role required: admin, security, user, backup-operator, or none.

system upgrade

`system upgrade` *`file`*
Upgrade the Data Domain system software from the *file* specified in the `/ddvar/releases` directory. The `upgrade` command shuts down the filesystem and reboots the

Data Domain system. The `upgrade` command may require over an hour, depending on the amount of data on the system. See the *EMC Data Domain Operating System Release Notes* for instructions on upgrading Data Domain systems. Role required: admin.

`system upgrade continue`
If upgrading a multi-node cluster, run this command option on the master controller to complete the second phase of the upgrade procedure. (Multi-node clusters, or "Global Deduplication Arrays," are deprecated as of this release. See the *EMC Data Domain Operating System Release Notes* for details.) Role required: admin.

`system upgrade history`
Display history of system upgrades. Role required: admin.

`system upgrade precheck` *`file`*
Check if current Data Domain operating system can be upgraded to the specified *file* in the `/ddvar/release` directory. Role required: admin.

`system upgrade status`
Display current status and phase of the upgrade procedure. This command option shows only the current status and then terminates. Users cannot monitor, or watch, upgrade progress. When the upgrade is finished, a message displays the time of completion. If upgrading from an earlier release (pre-5.2), this command becomes available after the system reboots. Role required: admin.

CHAPTER 34

user

The `user` command adds and deletes users, manages password aging and strength policies, and displays user roles. A role determines the type of operations a user can perform on the Data Domain system. See the *EMC Data Domain Operating System Administration Guide* for details.

The default administrative account is sysadmin. You can change the sysadmin password but cannot delete the account.

This chapter contains the following topics:

user Change History

This section provides a list of changes since the 5.4 release, for all 5.5.x releases, in order of most recent release to first release.

Modified Arguments in DD OS 5.5

user add *user* [role {admin | security | user | backup-operator | none}] [min-days-between-change *days*] [max-days-between-change *days*] [warn-days-before-expire *days*] [disable-daysafter-expire *days*] [disable-date *date*]

The *data-access* role is changed to *none*.

Modified Output in DD OS 5.5

user show list

This command now indicates the users who also have tenant-admin or tenant-user roles.

user show detailed [*user*]

This command now displays any tenant-unit roles that apply to the specified user.

Modified Behavior in DD OS 5.5

user del *user*

This command cannot be used to delete a DD Boost user. Delete the DD Boost user first, then use this command to delete the user name.

user reset

This command does not delete VDISK user accounts.

user show active

This command is now available to users with tenant-admin or tenant-user roles.

user change password [*user*]

This command is now available to users with tenant-admin or tenant-user roles.

user Guidelines and Restrictions

Unless otherwise noted, command options are available only to users with admin role permissions.

user add

user add *user* [role {admin | security | user | backup-operator | none}] [min-days-between-change *days*] [max-days-between-change *days*] [warn-days-before-expire *days*] [disable-days-after-expire *days*] [disable-date *date*]

Add a new user. A user name must start with a number or a letter. Special characters cannot be used. The user names **root** and **test** are default names on each Data Domain system and are not available for general use.

Admin-role users can create users with the **admin**, **user**, **backup operator**, and **none** roles. The default *sysadmin* user can create the first security officer role. After the first security-role user is created, only security-role users can add or delete other security-role users. After creating a security role, you must enable security authorization using the

`authorization policy` command. See the *EMC Data Domain Operating System Administration Guide* for details on user roles.

Argument Definitions

disable-date
Account is disabled on this date. If not specified, account never expires.

disable-days-after-expire
Account is disabled if inactive for the specified number of days past expiration.

max-days-between-change
Maximum number of days before password expires.

min-days-between-change
Minimum number of days allowed before the password can be changed again.

role
The type of user permissions allowed. The default role is `none`. See the *EMC Data Domain Operating System Administration Guide* for details.

warn-days-before-expire
Number of days of warning before a password expires.

user change

`user change password [user]`
Change the password of a user. Admin-role users can change the password for any user, and security-role users can change the passwords for other security role users. Users in all other management roles can change only their own passwords. Passwords must comply with the password strength policy, which you can check with the command option `user password strength show`. Role required: admin, tenant-admin, security, user, tenant-user, backup-operator, or none.

`user change role user {admin | user | backup-operator | none}`
Change the role of a user. Only admin-role users can change the role of other users. No management role is permitted to change the role of a security-role user. See the *EMC Data Domain Operating System Administration Guide* for more information on user roles.

user del

`user del user`
Remove any user except sysadmin and DD Boost users. The sysadmin user cannot be deleted. To delete a user name in use by DD Boost, delete the DD Boost user first, then use this command to delete the user name. Admin role users can delete users in all management roles except the security role. Security-role users can delete only security-role users.

Example 135

```
# user del ddboost1
o   ddboost1 cannot be deleted if referenced by ddboost
```

user disable

`user disable user`

Disable the specified user account so that the user cannot log on to the Data Domain system. Admin-role users can disable users in all management roles except the security role. Security-role users can only disable security-role users.

user enable

`user enable` *user* `[disable-date` *date*`]`

Enable the specified user account so that the user can log on to the Data Domain system. Admin-role users can enable users in all management roles except the security role. Security-role users can only enable security-role users.

user password

`user password aging option reset {all | [min-days-between-change] [max-days-between-change] [warn-days-before-expire] [disable-days-after-expire]}`

Reset one or more rules in the default password aging policy to the current default values. New accounts inherit the policy in effect at the time they are created, unless you set different aging options with the `user add` command. Role required: admin.

`user password aging option set {[min-days-between-change` *days*`] [max-days-between-change` *days*`] [warn-days-before-expire` *days*`] [disable-days-after-expire` *days*`]}`

Set the default values for the password aging policy. Role required: admin.

`user password aging option show`

Display the default password aging policy. Role required: admin.

`user password aging reset` *user* `{all | [min-days-between-change] [max-days-between-change] [warn-days-before-expire] [disable-days-after-expire]}`

Reset one or more rules in the password aging policy for the specified *user* to the current default values. Role required: admin for all except security-role users, security for security-role users.

`user password aging set` *user* `[min-days-between-change` *days*`] [max-days-between-change` *days*`] [warn-days-before-expire` *days*`] [disable-days-after-expire` *days*`]`

Set the password aging policy for the specified *user*. Role required: admin for all except security-role users, security for security-role users.

`user password aging show [`*user*`]`

Show the password aging policy for all users, or for a specified *user*. Only admin-role and security-role users can display the policy for other users. User-role, backup-operator-role, and none-role users can check the policy for only their own account.

`user password strength reset {all | min-length | min-char-classes}`

Reset the password strength policy to the default values. Role required: admin.

Argument Definitions

all
: Reset both the minimum length and minimum number of character classes to 1.

min-length
: Reset the minimum number of characters in the password to 1.

min-char-classes
Reset the minimum number of character classes to 1.

`user password strength set {[min-length` *`length`*`] [min-char-classes` *`num_classes`*`]}`
Set the password strength policy. Specify either min-length or min-char-classes, or both. Role required: admin.

Argument Definitions

min-length
The minimum number of characters in the password. The range is 1 to 100; the default setting is 6.

min-char-classes
The minimum number of character classes. Specify 1, 2, 3, or 4. Valid passwords must contain at least one character from the specified number of classes. The four character classes are lowercase letters, uppercase letters, digits, and special characters.

When DD OS counts the number of character classes, an uppercase letter at the beginning of the password does not count as an uppercase letter. Similarly, a digit at the end of the password does not count as a digit.

`user password strength show`
Show the current password strength policy. Role required: admin, security, user, backup-operator, or none.

user reset

`user reset`
This command deletes all user accounts except *sysadmin* and user accounts for security, DD Boost (role = none), and VDISK. This command also resets the password strength and password aging options to the factory default values. Role required: admin.

Note

This command option is not allowed on Retention Lock Compliance systems.

user show

`user show active`
Display a list of users currently logged in. Role required: admin, tenant-admin, security, user, tenant-user, backup-operator, or none.

Example 136

```
# user show active
User list from node "localhost".
Name       Idle   Login Time         Login From                  tty
--------   ----   ----------------   -------------------------   -----
sysadmin   0s     Tue Apr 22 12:25   test.test.com               pts/1
--------   ----   ----------------   -------------------------   -----
1 users found.
```

`user show detailed [`*`user`*`]`

Show detailed information for a specified user or for all users. Role required: admin or security.

Example 137

```
# user show detailed Tu1
User:                                    Tu1
Uid:                                     501
Role:                                    user
Last Login From:                         <unknown>
Last Login Time:                         Mon Jan 14 11:55:49 2013
Status:                                  enabled
Password Last Changed:                   Mar 16, 2006
Disable Date:                            never
Minimum Days Between Password Change:    0
Maximum Days Between Password Change:    99999
Warning Days Between Password Change:    7
Disable Days After Expire:               never
Tenant-unit Roles:
    Tenant-unit          Role
    -----------          -----
    Tenant-unit1         tenant-admin
    Tenant-unit2         tenant-user
```

`user show list`

Display list of system users. Role required: admin or security.

Figure 1 Output: user show list

```
sysadmin@DD2500-39# user show list
User list from node "localhost".
Name       Uid   Role    Last Login From           Last Login Time           Status    Disable Date
--------   ---   -----   -----------------------   -----------------------   -------   ------------
sysadmin   100   admin   carvej-dl.datadomain.com  Wed Mar 18 11:01:35 2015  enabled   never
--------   ---   -----   -----------------------   -----------------------   -------   ------------
1 users found.
```

CHAPTER 35

vdisk

The `vdisk` command creates and manages virtual disk devices that can be exported as a block-level disk device to an initiator over a Fibre Channel link. These block-level devices can be accessed by an application host, backup host, or a disk sub-system for block-level backup and recovery.

This chapter contains the following topics:

vdisk Change History

This section provides a list of changes since the 5.4 release, for all 5.5.x releases, in order of the most recent release to the first release.

New Commands in DD OS 5.5
The vdisk commands are a new feature in the DD OS 5.5 release.

vdisk Guidelines and Restrictions

- In the current release, virtual disks are only supported for certain solutions that incorporate EMC Data Domain and EMC Symmetrix VMAX systems. See the *Backup Compatibility Guide, EMC Data Domain Operating System 5.5* for information about supported configurations.
- If you use virtual disks, using either the VTL feature or DD Boost over Fibre Channel on the same Data Domain system is not supported.
- The output of `filesys show compression` may be misleading for virtual disks. Large virtual disks that contain very little data may show a total compression factor of 100%. This happens because, when you create a virtual disk, the system creates a file of the specified size (such as 2 PB) but does not actually write data to the disk, so no physical space is used. The compression ratio for that file will be extremely high until a substantial amount of real data gets written to the virtual disk.
- The output of `filesys show space` may also be misleading for virtual disks. When you create a virtual disk, the entire amount of space allocated for that virtual disk gets added to the `pre-comp` statistic for the file system. Likewise, when you delete a virtual disk, only the amount of space actually used for data gets added to the `Cleanable` statistic. This behavior is expected.
- Deleting the vdisk device that is assigned to LUN 0 from a vdisk device group is not supported, and will cause the other devices in the group to not be visible on the initiator.
- LUN 0 must be visible to all endpoints.

vdisk device

Manage individual virtual disk devices. A virtual disk device is a virtualized hard disk drive that has the characteristics of a physical hard disk drive: heads, cylinders, and sectors-per-track.

`vdisk device create [count` *`count`*`] capacity` *`n`* `{MiB|GiB|TiB|PiB} pool` *`pool-name`* `device-group` *`device-group-name`*

`vdisk device create [count` *`count`*`] heads` *`head-count`* `cylinders` *`cylinder-count`* `sectors-per-track` *`sector-count`* `pool` *`pool-name`* `device-group` *`device-group-name`*
Add one or more new virtual disk devices. You can specify the disk size either by entering a value *n* and a unit of size, or by specifying the physical characteristics of the virtual disk. Role required: admin.

`vdisk device destroy` *`device-name`* `[destroy-static-images {yes|no}]`
Delete a device and optionally delete its static images.

If you do not delete the static images, they become detached from (no longer associated with) the device. Use the vdisk static-image on page 309 commands to attach and detach static images. Role required: admin.

Example 138

```
vdisk device create count 2 capacity 10 GiB pool p1 device-group dg1
    Created VDISK device "vdisk-dev1", WWN: 60:02:18:80:00:00:00:00:63:05:1C:1B:02:D0:00:00
    Created VDISK device "vdisk-dev2", WWN: 60:02:18:80:00:00:00:00:63:05:1C:1B:02:D0:00:01
    2 VDISK devices created.
```

`vdisk device overwrite` *`device-name`* `[source-device` *`device-name`* `| source-pool` *`pool-name`* `source-device-group` *`device-group-name`*`] source-static-image` *`static-image-name`*

Overwrite a virtual disk device from a static-image. This command option destroys the existing data on the *device-name*. Role required: admin.

`vdisk device show detailed [`*`device-spec`*`] [pool` *`pool-name`* `[device-group` *`device-group-name`*`]]`

Show detailed information about all or selected virtual disk devices. All users may run this command option.

`vdisk device show list [`*`device-spec`*`] [pool` *`pool-name`*`] [device-group` *`device-group-name`*`]`

List all or selected virtual disk devices. All users may run this command option.

Argument Definitions

capacity *n* **[{MiB|GiB|TiB|PiB}]**
The capacity limit of the vdisk device. The default units are `GiB`. Enter a value and optionally specify the units. The capacity must be between 1 GiB and 4 TiB.

count *count*
The number of vdisk devices to create. The maximum is 2048. The default is 1.

cylinders *cylinder-count*
The number of cylinders that define the disk geometry, which is used to calculate the disk capacity.

destroy-static-images {yes|no}
Whether to delete the static images of the specified device.

device-group-name
A virtual disk device group name of up to 32 characters.

device-name
The name of the virtual disk device.

heads *head-count*
The number of heads that define the disk geometry, which is used to calculate the disk capacity.

pool-name
A virtual disk pool name of up to 32 characters.

sectors-per-track *sector-count*
The number of sectors per track that defines the virtual disk device geometry, which is used to calculate the disk capacity.

static-image-name
The name of a static image.

vdisk device-group

Manage virtual disk device groups.

A virtual disk device-group is a second-level container in a pool. It contains one or more virtual disk devices. It is represented as a subdirectory in the MTree of a virtual disk pool. The name space for a device-group name is limited to the MTree of a single vdisk pool.

Note

A device-group is not an access group.

A device group may contain:

- Devices
- Static images

`vdisk device-group create` *`device-group-name`* `pool` *`pool-name`*
Create a device-group in a local pool. Role required: admin.

`vdisk device-group destroy` *`device-group-name`* `pool` *`pool-name`*
Destroy a device-group, including all of its devices and data. Role required: admin.

`vdisk device-group rename` *`src-device-group-name destination-group-name`* `pool` *`pool-name`*
Rename the device-group *src-device-group-name* to *destination-group-name*. Role required: admin.

`vdisk device-group show detailed [`*`device-group-spec`*`] [pool` *`pool-spec`*`]`
Show detailed information about all or selected device-groups. All users may run this command option.

`vdisk device-group show list [`*`device-group-spec`*`]`
List all or selected device groups. The output shows the name of the pool that contains these device-groups and the number of devices in each device-group. All users may run this command option.

Argument Definitions

device-group-name
A virtual disk device group name of up to 32 characters.

device-group-spec
A list of virtual disk device groups that uses wildcards, such as “dg*”.

pool-name
A virtual disk pool name of up to 32 characters.

pool-spec
A list of virtual disk pools that uses a wildcard, such as “vpool*”.

vdisk disable

`vdisk disable`
Disable the vdisk service. Role required: admin.

vdisk enable

`vdisk enable`
Enable the vdisk service. Role required: admin.

vdisk group

Manage access between virtual devices and initiators.

Note

Use the `scsitarget group` commands to create, rename, or destroy virtual disk groups.

`vdisk group add` *`group-name`* `initiator` *`initiator-spec`*
Add an initiator to a virtual disk access group. Role required: admin.

`vdisk group add` *`group-name`* `{device` *`device-spec`* `| pool` *`pool-name`* `device-group` *`device-group-name`* `[device` *`device-spec`*`]} [lun` *`lun`*`] [primary-endpoint {all | none |` *`endpoint-list`*`}] [secondary-endpoint {all | none |` *`endpoint-list`*`}]`
Add virtual disk devices to a virtual disk access group. Role required: admin.

`vdisk group del` *`group-name`* `{device` *`device-spec`* `| initiator` *`initiator-spec`* `| pool` *`pool-name`* `device-group` *`device-group-name`* `[device` *`device-spec`*`]}`
Remove virtual disk devices from a virtual disk access group. Role required: admin.

`vdisk group modify` *`group-name`* `{device` *`device-spec`* `| pool` *`pool-name`* `device-group` *`device-group-name`* `[device` *`device-spec`*`]} [lun` *`lun`*`] [primary-endpoint {all | none |` *`endpoint-list`*`}] [secondary-endpoint {all | none |` *`endpoint-list`*`}]`
Modify the virtual disk device attributes in a virtual disk access group. Role required: admin.

`vdisk group use` *`group-name`* `{device` *`device-spec`* `| pool` *`pool-name`* `device-group` *`device-group`* `[device` *`device-spec`*`]} {primary | secondary}`
Switch the in-use endpoints list for one or more devices in a virtual disk access group between the primary port and the secondary endpoints. If you do not want to operate on all of the devices in the *device-group*, filter the devices by providing a *device-spec.* Role required: admin.

Argument Definitions

device-group-name
A virtual disk device group name of up to 32 characters.

device ***device-spec***
A list of devices that uses wildcards, such as “vdisk-dev*”.

group-spec
A list of virtual disk access groups that uses a wildcard, such as “group*”.

endpoint-list
A list of endpoints (logical names for target ports on the EMC Data domain system).

group-name
Name of an access group.

group-spec
A list of virtual disk access groups that uses a wildcard, such as “group*”.

initiator *initiator-spec*
A list of initiators attached to the EMC Data Domain system for the virtual disk service that uses a wildcard, such as “init1*”.

lun *lun*
A logical unit identified by a number. These are virtual disk devices exported from the EMC Data Domain system.

pool-name
A virtual disk pool name of up to 32 characters.

vdisk pool

Manage the virtual disk pool.

A virtual disk pool is the highest-level container for virtual disk objects. It corresponds to a managed tree (MTree) on an EMC Data Domain system.

Pools contain these lower-level objects:

- Device groups
- Devices
- Static images

`vdisk pool create` *`pool-name`* `user` *`user-name`*
Create a pool and its MTree, and assign an existing virtual disk user to the new pool. Role required: admin.

`vdisk pool destroy` *`pool-name`*
Destroy a pool, including all of its devices and data. Role required: admin.

`vdisk pool modify` *`pool-name`* `user` *`user-name`*
Assign an existing virtual disk user to an existing pool. Role required: admin.

`vdisk pool rename` *`src-pool-name dst-pool-name`*
Rename a pool from *src-pool-name* to *dst-pool-name*. Role required: admin.

`vdisk pool show list [`*`pool-spec`*`]`
List all pools or selected pools. All users may run this command option.

`vdisk pool show detailed [`*`pool-spec`*`] [user` *`vdisk-user`*`]`
Show detailed information about some or all pools. All users may run this command option.

Argument Definitions

pool-name
A virtual disk pool name of up to 32 characters.

pool-spec
A list of virtual disk pools that uses a wildcard, such as “vpool*”.

user-name
An EMC Data Domain system user name with a specified role, such as backup operator.

vdisk-user
An authorized virtual disk user who is associated (registered) with a virtual disk pool. This user may manage all virtual disk objects that are associated with the pool.

vdisk property

Set or remove properties for pools, device groups, devices, and static images.

`vdisk property reset object-name` *`name`* `object-type pool {all | property-name` *`name`*`}`

`vdisk property reset object-name` *`name`* `object-type device-group pool` *`pool-name`* `{all | property-name` *`name`*`}`

`vdisk property reset object-name` *`name`* `object-type device {all | property-name` *`name`*`}`

`vdisk property reset object-name` *`name`* `object-type static-image {device` *`device-name`* `| device-group` *`device-group-name`* `pool` *`pool-name`*`}{all | property-name` *`name`*`}`

Reset properties for a virtual disk object. Role required: admin.

`vdisk property set object-name` *`name`* `object-type pool property-name` *`name`* `property-value` *`value`*

`vdisk property set object-name` *`name`* `object-type device-group pool` *`pool-name`* `property-name` *`name`* `property-value` *`value`*

`vdisk property set object-name` *`name`* `object-type device property-name` *`name`* `property-value` *`value`*

`vdisk property set object-name` *`name`* `object-type static-image {device` *`device-name`* `| device-group` *`device-group-name`* `pool` *`pool-name`*`} property-name` *`name`* `property-value` *`value`*

Set key-value pair properties for a virtual disk object. Role required: admin.

Example 139

```
# vdisk property set object-name pool_3 object-type pool property-name Department
property-value HR
VDISK property set for pool “pool_3”
```

Argument Definitions

device-group-name
A virtual disk device group name of up to 32 characters.

device-name
The name of the virtual disk device.

object-name ***name***
A virtual disk object name. Virtual disk objects include pools, device groups, devices, and static images.

pool-name
A virtual disk pool name of up to 32 characters.

property-name ***name***
A property for a virtual disk object, which can be used to identity the object. For example, a virtual disk pool named **`pool-1`** might have a property **`department`** with the value **`HR`**.

property-value ***value***
A value for a virtual disk object property.

vdisk reset

Reset detailed virtual disk statistics. Role required: admin.

`vdisk reset detailed-stats`

vdisk show

Display information about virtual disk configuration limits and I/O statistics.

`vdisk show config`
Show the vdisk configuration limits. Role required: admin.

Example 140

```
vdisk show config

Name                      Current   Maximum
------------------------  -------   ---------
Pools                     2         50
Device-groups per pool    -         1024
Device-groups             20        51200
Devices                   17        2048
Static images                       Unlimited
------------------------  -------   ---------
```

`vdisk show detailed-stats`
Display detailed statistics. Role required: admin.

`vdisk show stats [{pool` *`pool-name`* `| pool` *`pool-name`* `device-group` *`devgrp-spec`*`}] [device` *`device-spec`*`] [interval` *`interval`*`] [count` *`count`*`]`
Periodically list I/O statistics for one or more virtual disk devices. If no pools or device groups are specified, a single-line total for each specified *interval* is displayed. If *interval* is not specified, a single iteration of statistics is displayed. If *count* is specified, the specified *count* number of iterations for statistics are displayed. Role required: admin.

Example 141

```
vdisk show stats
Start Time: 09/03 14:09:53
Interval: 2
Device        Ops/s    Read    Read   Write   Write
                      Ops/s   KiB/s   Ops/s   KiB/s
-----------   -----   -----   -----   -----   -----
vdisk-dev1        0       0       0       0       0
vdisk-dev2        0       0       0       0       0
vdisk-dev3        0       0       0       0       0
vdisk-dev4        0       0       0       0       0
vdisk-dev5        0       0       0       0       0
vdisk-dev6        0       0       0       0       0
-----------   -----   -----   -----   -----   -----
```

Argument Definitions

count *count*
The number of iterations of statistics to display.

device *device-spec*
A list of devices that uses wildcards, such as “vdisk-dev*”.

device-group *devgrp-spec*
A collection of virtual disk devices.

endpoint-spec
A list of endpoints that uses a wildcard, such as “endpoint*”.

interval *interval*
A time window (waiting time) within which to show virtual disk I/O statistics for virtual disk devices

pool-name
A virtual disk pool name of up to 32 characters.

vdisk static-image

Manage static images for devices.

A static image is a point-in-time copy of data for a vdisk device. Static images are created within a device group. You can copy (but not move) static images to other device groups. When you create a static image, it has the same pre-compression size as the original vdisk device. As you create more static images, the pre-compression sizes of the static image files adds to the pre-compression size of the containing Mtree. Likewise, the compression ratio is affected by creating the static image files. This behavior means that you can set Mtree quotas based on the sizes of the devices and their associated static images.

A static image contains:

- A point-in-time copy of application data for a vdisk device.
- Additional metadata inserted by the vdisk feature.

`vdisk static-image attach` *`source-static-image-name`* `source-pool` *`pool-name`* `source-device-group` *`device-group-name`* `destination-device` *`device-name`*
Attach an existing static image to a specified destination device. This command fails if a static image is already attached to the specified destination device. Role required: admin.

The attach and detach command options let you organize static images by associating them with a specific device, device group, or pool. When a static image becomes detached, it is still available for use, but it is not visible if you run `vdisk static-image show` commands and you filter the output by device.

Attaching a static image to a device does not imply that the device is using the image, and does not alter the current set of active data. The `attach` operation only associates the static image with the device, for purposes of organizing the static images.

`vdisk static-image copy` *`src-static-image-name`* {`source-device` *`device-name`* | `source-pool` *`pool-name`* `source-device-group` *`device-group-name`*} {`destination-device` *`device-name`* | `destination-pool` *`pool-name`* `destination-device-group` *`device-group-name`*}
Copy an existing static image to a specified destination. Role required: admin.

`vdisk static-image create device` *`src-device-name`*[`destination-device` *`device-name`* | `destination-pool` *`pool-name`* `destination-device-group` *`device-group-name`*]
Create a new static image of a device and attach the static image to the same device, to a different device, or to a specified device group in a specified pool. Role required: admin.

`vdisk static-image destroy` *`static-image-name`* `[device` *`device-name`* `| pool` *`pool-name`* `device-group` *`device-group-name`*`]`
Role required: admin.

`vdisk static-image detach` *`static-image-name`* `device` *`device-name`*
Detach a static image from a device. Role required: admin.

`vdisk static-image show detailed [`*`static-image-spec`*`] [device` *`device-name`* `| pool` *`pool-name`* `[device-group` *`device-group`*`]`
Show detailed information about all or specified static images. All users may run this command option.

`vdisk static-image show list [`*`static-image-spec`*`] [device` *`device-name`* `| pool` *`pool-name`* `[device-group` *`device-group`*`]]`
List all or specified static images. All users may run this command option.

Argument Definitions

device-group
A collection of virtual disk devices that you can use to manage the devices as a group. Device groups exist in virtual disk pools. Device group namespaces are limited to the virtual disk pool that contains the device group. Device group names may be up to 32 characters in length. The maximum number of device groups per pool is 1024. The maximum number of device groups per system is 5120.

device-group-name
A virtual disk device group name of up to 32 characters.

device-name
The name of the virtual disk device.

pool-name
A virtual disk pool name of up to 32 characters.

src-static-image-name
The name of a static image that is the source for a copy operation. The system generates these names automatically; use `vdisk static-image show list` to see the names.

static-image-name
The name of a static image.

static-image-spec
A list of static image names that uses a wildcard (*).

vdisk status

`vdisk status`
Show the status of the vdisk service. The output shows whether the vdisk service is enabled or disabled; whether the vdisk process is running; and whether the system has a license for the vdisk feature. Role required: admin.

vdisk trace

Manage tracing for virtual disk groups, initiators, and other components.

`vdisk trace disable [component` *`component-list`*`]`
Disable tracing for all or specified components. Role required: admin.

`vdisk trace enable [component {all | component-list}] [level {all | high | medium | low}] [timeout {never | timeout-value-in-minutes}]`
Enable tracing for all or specified components. By default, tracing applies to all components. If you specify a component, tracing is limited to that component, where applicable. Role required: admin.

`vdisk trace show [component {all |component-list}]`
Show tracing for all or specified components. All users may run this command option.

Argument Definitions

component-list
Specify `all`, `default`, or specific vdisk components from this list: `abnormal`, `device-io`, `fs-op`, `hba`, `obj_mgmt`, `procmon`, `scsi-other`, `scsi-req`, `scsitgt`, `sms-op`, `sys-mgmt`, `threads`, and `work-item`. The `default` list is used by default.

level {all | high | medium | low}
Tracing level. The default is `medium`.

timeout-value-in-minutes
Timeout for tracing. The default timeout is 10 minutes.

vdisk user

Manages user privilege to access and perform tasks on virtual disks.

`vdisk user assign vdisk-user`
Let the specified users work with virtual disks. Separate each user name in *user-list* with a comma. Role required: admin.

`vdisk user unassign vdisk-user`
Revoke the permission for the specified users to work with virtual disks. Role required: admin.

`vdisk user show`
List the virtual disk users and the pools to which each user is assigned. All users may run this command option.

Argument Definitions

vdisk-user
An authorized virtual disk user who is associated (registered) with a virtual disk pool. This user may manage all virtual disk objects that are associated with the pool.

CHAPTER 36

vtl

EMC Data Domain Virtual Tape Library (VTL) is a licensed software option that enables backup applications to connect to and manage a Data Domain system running Extended Retention as a virtual tape library.

VTL pools are MTree-based (as of DD OS 5.2). Multiple MTrees let you more closely configure DD OS for data management. MTree-based pools allow MTree replication to be used instead of directory replication. Existing pools are backward compatible. You may create additional backward-compatible pools as needed. VTL pool-based replication is performed using MTree replication for MTree pools, and directory replication for backward-compatible pools.

MTree-specific attributes can be applied to each VTL pool individually instead of inheriting a common set of attributes from the default `/backup` MTree. These attributes include snapshots and snapshot schedules, compression information, and migration policies for Extended Retention.

In previous versions, user access to VTL pool data in `/backup` (`/data/col1/backup`) was performed mainly through an NFS or CIFS mount of `/backup` and was relatively unconstrained. This led to issues where VTL data was changed beneath the VTL process; for example, when deleting a pool or copying files manually, which caused unexpected behavior and inconsistencies.

With MTrees, users may continue to use and manage VTL with little or no difference when compared to versions 5.1 and earlier.

This chapter contains the following topics:

vtl Change History

This section provides a list of changes since the 5.4 release, for all 5.5.x releases, in order of the most recent release to the first release.

New Commands in DD OS 5.5

`vtl config export`
Exports a VTL configuration to a file pathname.

`vtl config import`
Imports a VTL configuration from a file pathname.

Modified Arguments in DD OS 5.5

`vtl option disable ... [vtl vtl]`
New argument `vtl` *vtl* enables each library to have different option values.

`vtl option enable ... [vtl vtl]`
New argument `vtl` *vtl* enables each library to have different option values.

`vtl option reset ... [vtl vtl]`
New argument `vtl` *vtl* enables each library to have different option values.

`vtl option set ... [vtl vtl]`
New argument `vtl` *vtl* enables each library to have different option values.

`vtl option show ... [vtl vtl]`
New argument `vtl` *vtl* enables each library to have different option values.

Deprecated Commands in DD OS 5.5

`vtl option ... loop-id ...`
The use of `loop-id` with any of the `vtl option` commands is deprecated. To set the loop ID, enter a number between 1 and 26 in the *value* field of `scsitarget transport option set`.

`vtl reset hba`
See `scsitarget endpoint connection-reset all`.

vtl Guidelines and Restrictions

- Verify that at least one Fibre Channel (FC) interface card is installed on your Data Domain system. The VTL feature communicates between a backup server and a Data Domain system through an FC interface.
- The file system and scsitarget features must be enabled to run VTL.
- The recommended minimum record (block) size, which you must set for backup software on the application host, is 64 KiB or larger. Changing the block size after the initial configuration may render data written in the original size unreadable.
- The recommended number of concurrent virtual tape drive instances is platform-dependent, as is the recommended number of streams between a Data Domain system and a backup server. This number is system-wide and includes streams from all sources, such as VTL, NFS, and CIFS. For details on the number of tape drives and data streams, see the *EMC Data Domain Operating System Administration Guide*.
- The Data Domain VTL feature does not protect virtual tapes from a `filesys destroy`, which will delete all virtual tapes.

- The number of tapes that can be imported at one time is limited by:
  - The number of empty slots. You cannot import more tapes than the number of currently empty slots.
  - The number of slots that are empty and not reserved for a tape currently in a drive.
  - If a tape is in a drive and the tape origin is known to be a slot, the slot is reserved.
  - If a tape is in a drive and the tape origin is unknown (slot or CAP), a slot is reserved.
  - A tape that is known to have come from a CAP and that is in a drive does not get a reserved slot. (The tape returns to the CAP when removed from the drive.)
- The number of tapes that can be imported equals:
  - The number of empty slots.
  - The number of tapes that came from slots.
  - The number of tapes of unknown origin.

vtl add

`vtl add` *`vtl`* `[model` *`model`*`] [slots` *`num-slots`*`] [caps` *`num-caps`*`]`
Add a tape library. EMC Data Domain VTL supports a maximum of 64 library instances.

Role required: admin.

Argument Definitions

caps *num-caps*
Specifies the number of cartridge-access ports. The default is zero (0), and the maximum is 100 per library or 1000 per system.

model *model*
Specifies the name of the tape library model. See the Data Domain technical note for the model name that corresponds with your backup software.

slots *num-slots*
Specifies the number of slots in the library. You cannot add more drives than the number of configured slots. The maximum number of slots for all VTLs on a Data Domain system is 32,000. The default is 20 slots.

vtl
Specifies the name of the particular virtual tape library.

vtl cap

`vtl cap add` *`vtl`* `[count` *`num-caps`*`]`
Add cartridge access ports (CAPs) to a virtual tape library (VTL). The total number of CAPs cannot exceed 100 per library or 1000 per system.

Role required: admin.

`vtl cap del` *`vtl`* `[count` *`num-to-del`*`]`
Delete *num-to-del* CAPs from a VTL. The CAPs are deleted from the end.

Role required: admin.

To delete CAPs 8-10 on a VTL with 10 CAPs:

```
# vtl cap del vtl1 count 3
```

Argument Definitions

count *num-caps*
Specifies the number of cartridge-access ports to add. The default is 1.

count *num-to-del*
Specifies the number of objects to delete. The default is 1.

vtl
Specifies the name of the particular virtual tape library.

vtl config

`vtl config export [vtl vtl] output-file filename`
Export a VTL configuration to a file pathname.

Role required: admin.

`vtl config import [vtl vtl] [check-only] [skip-initiators] [retain-serial-numbers] [on-error {continue | stop}] input-file filename`
Import a VTL configuration from a file pathname.

Role required: admin.

Argument Definitions

check-only

This option:

- Uses the schema to validate the XML Configuration File.
- Validates the names of the following:
  - groups
  - initiators
  - endpoints
  - devices (changers, drives)
- Checks the format of the initiator system name.
- Checks whether the initiator_address_method element value belongs to one of the following:
  - SCSITGTD_INITIATOR_ADDRESS_METHOD_UNKNOWN
  - SCSITGTD_INITIATOR_ADDRESS_METHOD_AUTO
  - SCSITGTD_INITIATOR_ADDRESS_METHOD_VSA
- Checks whether the initiator_transport and endpoint_transport elements values belong to one of the following:
  - SCSITGTD_TRANSPORT_UNKNOWN
  - SCSITGTD_TRANSPORT_FC
  - SCSITGTD_TRANSPORT_FCOE
  - SCSITGTD_TRANSPORT_ISCSI
  - SCSITGTD_TRANSPORT_DUMMY
  - SCSITGTD_TRANSPORT_ALL
- Checks that the values of the following elements are BOOLEAN values (0,1 which mean FALSE and TRUE, respectively.)
  - endpoint_enabled_status
  - endpoint_online_status
  - auto_offline_option (global)
  - auto_eject_option (global)
  - vtl_auto_eject_option
  - vtl_auto_offline_option
- Validates the drive numbers.
  - Checks for repeated occurrences of the drive number.
  - Checks to make sure that the drive number does not exceed the maximum drive number allowed on the Data Domain system.
- Makes sure that the value of the VTL barcode length is appropriate, based on the model of the library.
- Does not commit the transactions or does not import any of the VTL configuration.
- When the retain-serial-numbers option is used, checks for the following:
  - whether the Data Domain system on which the `vtl config import retain-serial-numbers` is being used already has some VTL devices. If yes, it gives you an error.
  - validates the devices serial numbers.

input-file *filename*

Specifies the input file. Note that:

- The filename will be automatically appended with an .xml extension and stored in the /ddvar/etc/vtl_configuration_files directory.
- An .xml extension can also be provided explicitly. Any other extension will cause an error.

on-error {continue | stop}

Indicates what to do when an error occurs. For *stop*, the command stops, and all of the VTL configurations imported prior to the error remains, but no additional configurations are imported.

For *continue*, the action depends on the item being modified:

- Groups
  - If an error occurs while creating a group, and the group already exists, the command continues to create the next group.
  - For any other errors, the process stops.
- Endpoints
  - If an error occurs while renaming an endpoint, the command continues to configure the next endpoint.
- Initiators
  - If an error occurs while renaming an initiator, or setting an initiator alias, the command continues to configure the next initiator.
  - If an error occurs while adding an initiator to a group, the command continues to configure the next initiator.
- VTL-specific library options
  - If an error occurs while configuring any of the options, the command continues to configure the next option.
- Devices
  - Changers
    - If an error occurs while creating a changer, the command continues to configure the next VTL.
    - If an error occurs while adding a changer to a group, the command continues to add the changer to other groups.
  - Drives
    - If an error occurs while adding a drive, the command continues to add the next drive.
    - If an error occurs while adding a drive to a group, the command continues to add the drive to other groups.
- Options
  - If an error occurs while enabling/disabling a VTL option, the command continues to configure the next option.

output-file *filename*
Specifies the output file. Note that:

- The filename will be automatically appended with an .xml extension and stored in the /ddr/var/etc/vtl_configuration_files directory.
- An .xml extension can also be provided explicitly. Any other extension will cause an error.

retain-serial-numbers
Lets you preserve serial numbers while creating devices on a Data Domain system, but only when there are no pre-existing devices on that Data Domain system. If the serial number of a device is changed in the XML configuration file, then the vdev_id of that device should also be changed to an appropriate value, because the serial number of a device is dependent on the vdev_id.

skip-initiators
Lets you:

- Skip renaming initiators, if initiators with the same system names already exist.
- Skip setting initiator aliases.
- Skip adding initiators to groups.

vtl
Specifies the name of the particular virtual tape library.

vtl debug

`vtl debug disable [component {all | user | default | component-list}]`
Disable debug functionality of the specified components.

Role required: admin.

`vtl debug enable [component {all | user | default | component-list}] [level {high | medium | low}] [timeout {never | timeout-value-in-minutes}]`
Enable debug functionality for the specified components in persistent mode or for a specified `timeout` period (in minutes) at a specified debug `level`.

Role required: admin.

`vtl debug show [component {all | user | default | component-list}]`
Show specified components, or all components, running debug functionality.

Role required: admin, security, user, backup-operator, none.

Argument Definitions

component {all | user | default | *component-list*}
Specifies VTL debugging components. If you want to list them, you can include one or more of the following:

`vhba`

`scst`

`fc`

`ddcl`

`vtc`

`vmc`

`vtlprocess`

`group`

`vscsi`

`vtlsm`

`vtc_readahead`

`info_cache`

`persistent_reservations`

`master_client`

`master_server`

`worker_client`

`worker_server`

`vdev_thread`

`registry`

`misc`

Note

Components `master_client`, `master_server`, `worker_client`, and `worker_server` are used only for GDA, which is no longer supported as of 5.4.

level {high | medium | low}
Specifies the degree of VTL debugging verbosity.

timeout {never | *timeout-value-in-minutes*}
Determines the length of time (in minutes, if specified) that debugging should remain enabled for the specified components.

vtl del

`vtl del` *`vtl`*

Remove an existing VTL. Any tapes loaded into the library when the library is deleted are not destroyed. Instead, tapes are placed back into the virtual tape vault.

Role required: admin.

Argument Definitions

vtl
Specifies the name of the particular virtual tape library.

vtl disable

`vtl disable`
Close all libraries and shut down the VTL process.

Role required: admin.

vtl drive

`vtl drive add` *`vtl`* `[count` *`num-drives`*`] [model` *`model`*`]`
Add drives to a VTL. Drives are added by starting with drive number 1 and scanning for logical unit address gaps left by `vtl drive del`. When the gaps are filled, the drives are appended to the end of the library. The number of slots within a library cannot be fewer than the number of drives in the library. If an attempt is made to add more drives than the current number of slots, the system automatically adds the additional slots required. Be aware that you cannot mix drive models within the same library.

Role required: admin.

`vtl drive del` *`vtl`* `drive` *`drive-number`* `[count` *`num-to-del`*`]`
Delete virtual drives from a VTL. Any drive can be deleted, which means there can be gaps in the drive list. This may cause issues with some applications.

Role required: admin.

`vtl drive show {serial-number` *`serial-number`* `| vtl` *`vtl`* `[drive {`*`drive-list`*`}]}`
View details of VTL drives.

Role required: admin, security, user, backup-operator, none.

Output Definitions

Location
Standard format location of library or drive.

Serial #
Drive serial number.

Vendor
Drive vendor identification.

Product
Drive product identification.

Product revision
Drive product revision.

Status
Drive status.

Barcode
Barcode of loaded tape.

Pool
Pool of loaded tape.

Previous Slot
Previous slot of loaded tape.

Device
SCSI device ID.

Persistent Reservation
Persistent reservation information.

Access Groups
Fibre Channel access groups for device.

Argument Definitions

count *num-drives*
Specifies the number of drives to add. The default is 1.

count *num-to-del*
Specifies the number of objects to delete. The default is 1.

drive *drive-list*
Specifies a list of drives.

drive *drive-number*
Specifies the number of the VTL drive.

model *model*
Specifies the name of the tape library model. See the Data Domain technical note for the model name that corresponds with your backup software.

serial-number *serial-number*
Specifies the serial number.

vtl
Specifies the name of the particular virtual tape library.

vtl enable

`vtl enable`
Enable the VTL subsystem.

Role required: admin.

vtl export

`vtl export` *`vtl`* `{slot | drive | cap}` *`address`* `[count` *`count`*`]`
Remove tapes from a slot, drive, or cartridge-access port (CAP) and send them to the vault.

Role required: admin backup-operator.

Argument Definitions

address
Specifies the address.

count *count*
Specifies the number of tapes.

vtl
Specifies the name of the particular virtual tape library.

vtl group

Before using `vtl group`, note the following about VTL groups:

- The name for a VTL group must be unique. It can contain only the characters 0-9, a-z, A-Z, underscore, and hyphen, and it cannot exceed 256 characters.
- These names are reserved and cannot be used: TapeServer, default, all, and summary.
- A maximum of 2,048 groups is allowed.
- Clients can access only selected LUNs from a Data Domain system.
- VTL group changes may require the media server to rescan the SCSI bus, or you can reset the link with `scsitarget endpoint connection-reset`.
- In the event of path failure, you can run `vtl group use` to switch between the primary and secondary port lists. To return the group to the primary port list after the path is repaired, run `vtl group use primary`.

`vtl group add` *`group-name`* `initiator` *`initiator-alias-or –WWPN`*
Add an initiator alias or world-wide port name to the specified VTL access group.

Role required: admin.

`vtl group add` *`group-name`* `vtl` *`vtl-name`* `{all | changer | drive` *`drive-list`*`} [lun` *`lun`*`] [primary-port {all | none |` *`port-list`*`}] [secondary-port {all | none |` *`port-list`*`}]`
Add a changer or drives to the specified VTL access group. You can add a changer or drive, optionally starting at a given logical unit number (LUN). You can optionally specify primary and secondary Data Domain system VTL port lists. By default, the port lists contain all Data Domain system VTL ports.

Role required: admin.

`vtl group create` *`group-name`*
Create a VTL access group with the specified group name. After the group is created, VTL devices (changer or drive) and initiators may then be added to the group.

Role required: admin.

`vtl group del` *`group-name`* `initiator` *`initiator-alias-or-WWPN`*
Remove an initiator alias or world-wide port name from the specified VTL access group.

Role required: admin.

`vtl group del` *`group-name`* `vtl` *`vtl-name`* `{all | changer | drive` *`drive-list`*`}`
Remove one or more devices from a group. This immediately removes access from the specified initiator to the VTL devices within the group.

Role required: admin.

`vtl group destroy` *`group-name`*
Remove the specified empty VTL access group. Before you can destroy a group, run `vtl group del` to remove the initiators and devices from the group.

Role required: admin.

`vtl group modify` *`group-name`* `vtl` *`vtl-name`* `{all | changer [lun` *`lun`*`] | drive` *`drive`* `[lun` *`lun`*`]} [primary-port {all | none |` *`port-list`*`}] secondary-port {all | none |` *`port-list`*`}]`

Modify a group without removing and replacing devices or initiators in the group. You can use this to change LUN assignments and primary and secondary port assignments. The main purpose of this command is to change group port assignments.

Role required: admin.

`vtl group rename` *`src-group-name dst-group-name`*

Rename a VTL access group. The *dst-group-name* must not already exist. Be aware that this does not interrupt active sessions.

Role required: admin.

`vtl group show [ all | vtl` *`vtl`* `|` *`group-name`* `]`

Show information about VTL access groups.

Role required: admin, security, user, backup-operator, none.

`vtl group use` *`group-name`* `[vtl` *`vtl-name`* `{all | changer | drive` *`drive-list`*`}] {primary | secondary}`

Switch ports in use for the specified changer in a group or library to the primary or secondary port list for the specified changer or drives. This immediately changes the access path to the primary or secondary port for the selected VTL components in an access group. When the path is restored, this will return the group to its primary port list. After you apply a group to new VTL ports, you may need to rescan the media server's SCSI bus. Also, a backup application may need to rescan available SCSI devices. This interrupts any current access to the specified group and is intended to be used during path failures.

Role required: admin.

Argument Definitions

drive ***drive-list***
: Specifies a list of drives.

dst-group-name
: Specifies the name of the destination group.

group-name
: Specifies the VTL access group. **`TapeServer`** is a reserved group and cannot contain initiators.

initiator initiator-alias-or-WWPN
: Specifies the initiator alias or world-wide port name.

lun ***lun***
: Specifies the device address to pass to the initiator. The maximum logical unit number (LUN) is 16383. A LUN must be unique within a group, but does not have to be unique across the system. LUNs for VTL devices within a group must start with zero (0) and be contiguous numbers.

port ***port-list***
: Lets you include a comma-separated list of Data Domain system VTL ports. You can specify port names as a range separated by a hyphen (-). The ports must already exist. For multiple ports, separate each name with a comma, and enclose the list with double quotes.

primary-port
: Specifies the primary VTL ports on which the devices are visible. By default, or if you specify `all`, the VTL devices are visible on all ports. Specify `none` if the devices should not be visible on any ports.

secondary-port
Specifies the secondary VTL ports on which devices are visible to `vtl group use secondary`. By default, the devices are visible on all ports. The secondary port list supports path redundancy.

src-group-name
Specifies the name of the source group.

vtl
Specifies the name of the particular virtual tape library.

vtl import

`vtl import` *`vtl`* `barcode` *`barcode`* `[count` *`count`*`] [pool` *`pool`*`] [element {drive | cap | slot}] [address` *`addr`*`]`
Move tapes from the vault into a slot, drive, or cartridge access port.

Use `vtl tape show` to display the total number of slots for a VTL and to view which slots are currently used. Use commands from the backup server to move VTL tapes to and from drives. Although `vtl import` can move tapes into tape drives, backup software commands from the backup server are more frequently used to move VTL tapes to and from drives. The default address is 1, the default element is slot, and the default pool is Default.

If no address is specified, the first free slot available is used. For example if slots 1 through 4 are occupied or reserved, the address used will be 5. If the address you specify is already in use, the first free slot that is larger than the address specified is used.

Role required: admin, backup-operator.

The following two commands are equivalent:

```
# vtl import VTL1 barcode TST010L1 count 5
```

```
# vtl import VTL1 barcode TST010L1 count 5 element slot
address 1
```

Argument Definitions

address
Specifies the address.

barcode *barcode*

Specifies an eight-character virtual tape identifier. The first six characters are numbers or uppercase letters (0-9, A-Z). The last two characters are the tape code for the supported tape type: L1 (LTO-1, 100 GiB, the default capacity), LA (LTO-1, 50 GiB), LB (LTO-1, 30 GiB), LC (LTO-1, 10 GiB), L2 (LTO-2, default capacity of 200 GiB), L3 (LTO-3, default capacity of 400 GiB), L4 (LTO-4, default capacity of 800 GiB), L5 (LTO-5, default capacity of 1.5 TiB).

The default capacities are used if you do not specify the *capacity* argument when creating the tape cartridge. If you do specify a capacity, it will override the two-character tag.

When using `count` and `barcode` together, use a wild card character in the barcode to make the count valid. An asterisk matches any character in that position and all other positions. A question mark matches any character in that position.

Note

L1, LA, LB and LC tapes cannot be written on LTO-3 tape drives. L2 and L3 tapes cannot be read on LTO-1 tape drives. Also, LTO-4 will not read L2 tapes (in addition to the LA-L1 tapes).

count *count*

Specifies the number of tapes.

element

Specifies the destination element.

pool *pool*

Specifies the name of the pool. This argument is required if tapes are in a pool.

vtl

Specifies the name of the particular virtual tape library.

vtl initiator

`vtl initiator reset address-method initiator` *`initiator-alias-or-WWPN`*

Reset, to the default (auto), the address method used when responding to a SCSI REPORT LUNS command.

Role required: admin.

`vtl initiator reset alias` *`alias-name`*

Remove an initiator alias. Reset (delete) the initiator alias from the system. Deleting the alias does not affect any VTL access from the specified initiator. To remove an initiator from a group, use `vtl group del` instead.

Role required: admin.

`vtl initiator set address-method {auto | vsa} initiator` *`initiator-alias-or-WWPN`*

Set the device address method used when responding to a SCSI REPORT LUNS command from the specified initiator. With most platforms, you do not need to change the default device address method. Use this to work around any platform-specific limitations you may encounter.

Role required: admin.

`vtl initiator set alias` *`alias-name`* `wwpn` *`wwpn`*

Add an initiator alias. This sets an alias for an initiator's WWPN (world-wide port name). An initiator is any Data Domain system client HBA's WWPN. This does not interrupt traffic or VTL group access.

Use `vtl initiator show` on the Data Domain system to list the client WWPNs detected by the Data Domain system. You must match the WWPNs in the command output to the client's HBA WWPN, including colon delimiters.

The alias must be unique, cannot exceed 256 characters, and can contain the characters 0-9, a-z, A-Z, underscore, and hyphen only. The maximum number of aliases is 128.

Role required: admin.

Example 142

The following example uses the client name and port number as the alias to avoid confusion with multiple clients that may have multiple ports:

```
# vtl initiator set alias client22_2a
```

`vtl initiator show [initiator` *`initiator-alias-or-WWPN`* `| port` *`port-list`*`]`

Display information about one or all Fibre Channel devices. Not all devices shown are initiators. Output returned includes Initiator, Group, Status, WWNN, WWPN, Port, Symbolic Port Name, and Address Method.

Role required: admin, security, user, backup-operator, none.

Argument Definitions

alias *alias*
: Specifies the alias.

auto
: Specifies the device address method chosen based on the numeric LUN range being reported. For 0 - 255, peripheral device addressing is used. For 256 - 16383, flat device addressing is used (default).

initiator initiator-alias-or-WWPN
: Specifies the initiator alias or world-wide port name.

port *port-list*
: Lets you include a comma-separated list of Data Domain system VTL ports. You can specify port names as a range separated by a hyphen (-). The ports must already exist. For multiple ports, separate each name with a comma, and enclose the list with double quotes.

vsa
: Enables volume set addressing (VSA). This method is used primarily for addressing virtual buses, targets, and LUNs. The HP-UX operating system selects the VSA method based on inquiry data and LUN information returned by the SCSI-3 `REPORT LUNS` command.

wwpn *wwpn*
: Specifies the world-wide port name.

vtl option

`vtl option disable` *`option name`* `[vtl` *`vtl`* `]`

Disable a VTL option. Optionally, you can do this only for the specified VTL.

Role required: admin.

`vtl option enable` *`option name`* `[vtl` *`vtl`* `]`
Enable a VTL option. Optionally, you can do this only for the specified VTL.

Role required: admin.

`vtl option reset` *`option name`* `[vtl` *`vtl`* `]`
Reset a VTL option to its default value. Optionally, you can do this only for the specified VTL.

Role required: admin.

`vtl option set` *`option name value`* `[vtl` *`vtl`* `]`
Set an option and value. Optionally, you can do this only for the specified VTL.

Role required: admin.

`vtl option show {`*`option name`* `| all} [vtl` *`vtl`*`]`
Show settings for a specific option, all VTL options, or only for the specified VTL.

Role required: admin, security, user, backup-operator, none.

Example 143

```
# vtl option show all vtl b12234
Name               Value
auto-eject         enabled
auto-offline       disabled
barcode-length     6
```

Argument Definitions

Values for *option name* are:

auto-eject
If enabled, tapes placed into CAPs are automatically ejected to the vault.

auto-offline
If enabled, tapes being moved from a drive causes the drive to be automatically taken offline and unloaded unless the **`prevent`** bit is set for the drive.

barcode-length
Allows you to explicitly set the length – to either 6 or 8 – of the tape barcode that the library will report to the initiator/client.

By default (when barcode-length is not set), the library reports the length of the barcode depending on the type of library. For example, if tape AAA001L3 is put in an L180, DDVTL, or RESTORER-L180 library, the library will report this tape to the initiator/client as AAA001. If the same tape is placed in a TS3500, I2000, or I6000 library, the library will report this tape to the initiator/client as AAA001L3.

However, if you do specify the barcode-length, for example, **`vtl option set barcode-length 6 vtl my_ts3500_library`** on a TS3500 library, then the barcode will be reported to the initiator/client as AAA001, which is the same length as for an L180 library.

loop-id - deprecated
The Fibre Channel loop ID: 1-26. This value has been deprecated and will be removed in future releases. To set the loop ID on a Data Domain system, enter a number between 1 and 26 in the *value* field of `scsitarget transport option set`.

vtl pool

`vtl pool add` *pool* [*backwards-compatibility-mode*]
Create a VTL pool. If `backwards-compatibility-mode` is used, a pool with backwards compatibility is created in the default directory (`/backup`). It is recommended that you create backwards-compatibility pools only if you have specific requirements, for example, replication with a pre-5.2 DD OS system. Replication of backwards-compatibility-mode pools is done using directory-based replication, as in previous releases.

Role required: admin.

`vtl pool del` *pool*
Delete a VTL pool. You must run `vtl tape del` to remove all tapes from a pool, or use `vtl tape move` to move all tapes to another pool.

Role required: admin.

`vtl pool rename` *src-pool dst-pool*
Rename a VTL pool. A pool can be renamed only if none of its tapes is in a library.

Role required: admin.

`vtl pool show {all |` *pool*`}`
List all tape pools or the contents of a specific *pool*. If `all` is used, a summary of all tape pools is provided, including the state of each pool, the number of tapes, the total usage and compression for each pool, whether a pool is a replication destination, the Retention Lock status of the pool, read/write properties, and the number of tapes in the pool.

Role required: admin, security, user, backup-operator, none.

Output Definitions

RW
Pool has normal read/write properties.

RD
Pool is a replication destination.

RO
Pool is read-only.

RLCE
Pool is Retention Lock Compliance Enabled.

RLGE
Pool is Retention Lock Governance Enabled.

RLGD
Pool is Retention Lock Governance Disabled.

BCM
Pool is in backwards-compatibility mode.

`vtl pool upgrade-to-mtree {`*pool-list* `| all} [check-only]`
Upgrade a VTL pool(s) to an MTree pool(s). If *pool-list* is specified, all pools in the list are candidates for upgrade. If `all` is specified, all backwards-compatibility mode pools are upgraded. If `check-only` is specified, the precheck is run, but no upgrade is performed, so that you can plan for these changes prior to the upgrade. If no arguments are provided, a check is made to see if an upgrade is necessary or possible. If so, the upgrade is performed, which converts the specified backwards-compatibility mode pools to MTree pools. An upgrade may be run only when VTL is disabled.

A directory pool will be converted to an MTree pool only if the following prerequisites are met:

- The directory pool must not be a replication source or destination.
- The file system must not be full.
- The file system must not have reached the maximum number of MTrees allowed (100).
- There must not already be an MTree with the same name.
- If the directory pool is being replicated to an older DD OS (for example, from DD OS 5.5 to DD OS 5.4), it cannot be converted. As a workaround:
  - Replicate the directory pool to a second Data Domain system.
  - Replicate the directory pool from the second Data Domain system to a third Data Domain system.
  - Remove the second and third Data Domain systems from the managing Data Domain system's Data Domain network.
  - On any of the systems running DD OS 5.5, run the `vtl pool upgrade-to-mtree` command.

See the *EMC Data Domain Operating System Administration Guide* for more information about upgrading directory pools to MTree pools.

Role required: admin.

Example 144

```
# vtl pool upgrade-to-mtree all
```

Example 145

```
# vtl pool upgrade-to-mtree old-pool check-only
```

Argument Definitions

dst-pool
Specifies the name of the new VTL pool.

source *src-pool*
Specifies the name of the current VTL pool.

vtl port

`vtl port disable {all | port-list}`
Disable a single Fibre Channel port or all Fibre Channel ports in the list.

Role required: admin.

`vtl port enable {all | port-list}`
Enable a single Fibre Channel port or all Fibre Channel ports in the list.

Role required: admin.

`vtl port option reset [{fcp2-retry | topology} [port {port-list | all}]]`
Reset options on VTL Fibre Channel ports.

Role required: admin.

`vtl port option set fcp2-retry {disable | enable} [port {port-list | all}]`
Set FCP2 retry on VTL Fibre Channel ports. Use this command only if FCP2 retry connectivity problems occur.

Role required: admin, security, user, backup-operator, none.

`vtl port option set topology {loop-preferred | loop-only | point-to-point} [port {port-list | all}]`
Set topology on VTL Fibre Channel ports.

Role required: admin.

`vtl port option show [{fcp2-retry | topology} [port {port-list | all}]]`
Show options on VTL Fibre Channel ports.

Role required: admin, security, user, backup-operator, none.

`vtl port show detailed-stats`
Show detailed information about Fibre Channel ports.

Role required: admin, security, user, backup-operator, none.

Output returned includes:

- Control commands
- Write commands
- Read commands
- In (number of MiB written--the binary equivalent of MB)
- Out (number of MiB read)
- Link failures
- LIP count
- Sync losses
- Signal losses
- Error count in primitive sequence protocol
- Number of invalid tx words
- Number of frames received with a bad CRC

`vtl port show hardware`
Show Fibre Channel ports hardware.

Role required: admin, security, user, backup-operator, none.

Output returned includes:

- Model
- Firmware
- WWNN
- WWPN

`vtl port show stats [port {port-list | all}] [interval secs] [count count]`
Show VTL I/O stats on Fibre Channel ports.

Role required: admin, security, user, backup-operator, none.

Output returned includes:

- Port
- ops/s
- Read KiB/s
- Write KiB/s
- Soft Errors
- Hard Errors

`vtl port show summary`
Show summary information about Fibre Channel ports.

Role required: admin, security, user, backup-operator, none.

Output returned includes:

- Port
- HBA slot
- HBA port
- Connection type
- Link speed
- Port ID
- Enabled
- Status

Argument Definitions

count *count*
Specifies the number of tapes.

detailed-stats
Provides detailed statistics.

fcp2-retry
Specifies the port option.

interval *secs*
Specifies the time interval in seconds.

loop-only
Specifies the port topology option.

loop-preferred
Specifies the port topology option.

point-to-point
Specifies the port topology option.

port *port-list*
Lets you include a comma-separated list of Data Domain system VTL ports. You can specify port names as a range separated by a hyphen (-). The ports must already exist. For multiple ports, separate each name with a comma, and enclose the list with double quotes.

summary
Shows a summary of all tapes and tape usage.

topology
Specifies the port option.

vtl readahead

`vtl readahead reset {stats | summary}`
Reset VTL readahead information. When VTL reads a tape file, it improves performance by reading ahead information from tape files and caching the information until needed.

Role required: admin.

`vtl readahead show {stats | detailed-stats | summary}`
Display readahead information about each open tape file that has been read.

Role required: admin, security, user, backup-operator, none.

Argument Definitions

detailed-stats
Provides detailed statistics.

stats
Displays statistics.

summary
Shows a summary of all tapes and tape usage.

vtl rename

`vtl rename` *`src-vtl dst-vtl`*
Rename a virtual tape library. The source name and the destination name must differ.

Role required: admin.

vtl reset

`vtl reset hba - deprecated`
This command is deprecated. Use `scsitarget endpoint connection-reset all` instead.

Role required: admin.

`vtl reset detailed-stats`
Reset the VTL detailed statistics.

Role required: admin.

vtl show

`vtl show config [`*`vtl`*`]`
Show the library name and model and tape drive model for a single VTL or all VTLs.

Role required: admin, security, user, backup-operator, none.

`vtl show detailed-stats`
Show a large quantity of detailed VTL statistics and information.

Role required: admin, security, user, backup-operator, none.

`vtl show element-address [`*`vtl`*`]`
Show the following information for all VTLs, or a single VTL:

- Starting element address
- Slot count and starting address
- CAP count and starting address
- Drive count and starting address
- Changer count and starting address

Role required: admin, security, user, backup-operator, none.

`vtl show stats [port {`*`port-list`*` | all}] [interval `*`secs`*`] [count `*`count`*`]`
Show VTL I/O stats.

Role required: admin, security, user, backup-operator, none.

`vtl show stats `*`vtl`*` [drive {`*`drive-list`*` | changer | all}] [port {`*`port-list`*` | all}] [interval `*`secs`*`] [count `*`count`*`]`
Show VTL I/O stats including detailed traffic statistics for devices belonging to the specified VTL. Statistics include speed of read/writes in KiB per second, per VTL drive. This information is available only if a *vtl* is specified. All users may run this command option.

Role required: admin, security, user, backup-operator, none.

Argument Definitions

count *count*
Specifies the number of tapes.

drive {*drive-list***| changer | all}**
Lets you include all drives, changer, or a list of drives.

detailed-stats
Provides detailed statistics.

interval *secs*
Specifies the time interval in seconds.

port {*port-list***| all}**
Lets you include all ports, or a comma-separated list of Data Domain system VTL ports. You can specify port names as a range separated by a hyphen (-). The ports must already exist. For multiple ports, separate each name with a comma, and enclose the list with double quotes.

vtl
Specifies the name of the particular virtual tape library.

vtl slot

`vtl slot add `*`vtl`*` [count `*`num-slots`*`]`
Add slots to a VTL. Additional slots are added to the end of the list of slots in the specified VTL. The maximum is 32,000 slots per library and 64,000 slots per system.

Role required: admin.

`vtl slot del `*`vtl`*` [count `*`num-to-del`*`]`
Delete one or more slots from a VTL.

Role required: admin.

Argument Definitions

count *num-slots*
Specifies the number of slots to add to the library. You cannot add more drives than the number of configured slots. The maximum number of slots for all VTLs on a Data Domain system is 32,000. The default is 20 slots.

count *num-to-del*
Specifies the number of slots to delete from the library.

vtl
Specifies the name of the particular virtual tape library.

vtl status

`vtl status`
Show the state of the VTL process.

Role required: admin, security, user, backup-operator, none.

vtl tape

`vtl tape add` *barcode* `[capacity` *capacity*`] [count` *count*`] [pool` *pool*`]`
Add one or more virtual tapes and insert them into the vault. Optionally, add the tapes to the specified pool.

Role required: admin.

`vtl tape copy barcode` *barcode* `[count` *count*`] source` *src-pool* `[snapshot` *src-snapshot*`] destination` *dst-pool*
Copy tapes between VTL pools. Note that an opened writable tape in a tape drive may not be copied. Additionally, source and destination pools cannot be the same unless copying from a snapshot. If the snapshot argument is specified, tapes are copied from the snapshot of the source pool. In this case, the destination pool can be the same as the source pool. A tape in the vault or library slot/cap, or opened read-only in a tape drive, can be copied. A tape that is opened writable in a tape drive may not be copied.

Role required: admin.

```
# vtl tape copy barcode AA0000LC count 100 source replica-dest
destination daily-restores
```

`vtl tape del` *barcode* `[count` *count*`] [pool` *pool*`]`
Delete the specified tape or one or more tapes. You cannot delete tapes that are in a VTL.

NOTICE

This command deletes all data on tapes.

Role required: admin.

`vtl tape history delete`
Delete all VTL tape history.

Role required: admin.

`vtl tape history disable`
Disable VTL tape history.

Role required: admin.

`vtl tape history enable`
Enable VTL tape history.

Role required: admin.

`vtl tape history show` *`barcode`* `[pool` *`pool`*`] [start-time` *`MMDDhhmm`*`[[`*`CC`*`]`*`YY`*`]] [end-time` *`MMDDhhmm`*`[[`*`CC`*`]`*`YY`*`]]`
Show history of move-related events for a given tape.

Role required: admin, security, user, backup-operator, none.

`vtl tape history status`
Show current state of the VTL tape history feature.

Role required: admin, security, user, backup-operator, none.

`vtl tape modify` *`barcode`* `[count` *`count`*`] [pool` *`pool`*`] retention-lock {`*`date`* `|` *`period`*`}`
Modify the state of retention lock of a specified tape or tapes. Change the amount of time to maintain the retention lock on the specified tape or tapes. If the volume is not mounted, the change is made immediately. Otherwise, data is synchronized first. This will fail if the file system is read-only.

Role required: admin.

`vtl tape modify` *`barcode`* `[count` *`count`*`] [pool` *`pool`*`] writeprotect {on | off}`
Set the write protect state of a specified tape. If the volume is not mounted, the tape file permission is changed immediately. Otherwise, outstanding writes are synchronized first.

Role required: admin.

`vtl tape move` *`vtl`* `source {slot | drive | cap} {`*`src-address-list`* `| all} destination {slot | drive | cap} {`*`dst-address-list`* `| auto}`
Move one or more tapes between elements in a VTL. Values for *src-address-list* include: all, 1, 2-14, 3-5, 7-10. Values for *dst-address-list* include: 1, 2-14, 3-5, 7-10, and auto.

You may specify the `auto` keyword only if moving from tapes from drives to slots. If `auto` is selected, VTL finds the previous slot the tape was in and moves it to that slot. If the slot is not empty, it moves the next available slot.

Role required: admin, backup-operator.

`vtl tape move barcode` *`barcode`* `[count` *`count`*`] source` *`src-pool`* `destination` *`dst-pool`*
Move a tape between VTL pools if it is in the vault, or in a library slot or CAP. It cannot be moved between VTL pools if the tape is open in a drive, or if it is one of the following kinds of tapes:

- Tapes open in a drive
- Tapes on a replica
- Tapes configured with Retention Lock

Role required: admin.

`vtl tape show {all | pool` *`pool`* `| vault |` *`vtl`*`} [summary] [count` *`count`*`] [barcode` *`barcode`*`] [time-display {modification | creation | retention}] [sort-by {barcode | pool | location | state | capacity | usage | percentfull | compression | time | modtime} [{ascending | descending}]]`

Display information about tapes, including modification, creation, or retention times. If `time-display` is omitted, the default is modification time for backward-compatibility-mode VTL pools.

Modification times used by the system for age-based policies may differ from the last modified time displayed in the tape information sections of the GUI and CLI. This is expected behavior.

If you are using Extended Retention, see the *EMC Data Domain Operating System Administration Guide* for details on modification time.

Role required: admin security, user, backup-operator, none.

Argument Definitions

address
Specifies the address.

barcode *barcode*
Specifies an eight-character virtual tape identifier. The first six characters are numbers or uppercase letters (0-9, A-Z). The last two characters are the tape code for the supported tape type: L1 (LTO-1, 100 GiB, the default capacity), LA (LTO-1, 50 GiB), LB (LTO-1, 30 GiB), LC (LTO-1, 10 GiB), L2 (LTO-2, default capacity of 200 GiB), L3 (LTO-3, default capacity of 400 GiB), L4 (LTO-4, default capacity of 800 GiB), L5 (LTO-5, default capacity of 1.5 TiB).

The default capacities are used if you do not specify the *capacity* argument when creating the tape cartridge. If you do specify a capacity, it will override the two-character tag.

When using `count` and `barcode` together, use a wild card character in the barcode to make the count valid. An asterisk matches any character in that position and all other positions. A question mark matches any character in that position.

Note

L1, LA, LB and LC tapes cannot be written on LTO-3 tape drives. L2 and L3 tapes cannot be read on LTO-1 tape drives. Also, LTO-4 will not read L2 tapes (in addition to the LA-L1 tapes).

capacity *capacity*
Specifies the number of gibibytes (GiB) for each tape created. This value overrides default barcode capacities. The upper limit is 4,000 GiB. For best results, when data becomes obsolete (and the Data Domain system cleaning process marks data for removal), set capacity to 100 or less for efficient reuse of Data Domain system disk space.

GiBs equal the base-2 value of Gigabytes (GB).

count *count*
Specifies the number of tapes.

pool *pool*
Specifies the name of the pool. This argument is required if tapes are in a pool.

snapshot *src-snapshot*
Describes a specific snapshot within a source pool.

source *src-pool*
Specifies the name of the current VTL pool.

write-protect {on | off}
Enables or disables write-protection for a tape.

APPENDIX A

Time Zones

This appendix covers the following topics:

Time Zones Overview

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

Locate your time zone using the following tables.

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

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

Examples of time zones include:

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

Africa

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

America

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

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

Antarctica

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

Asia

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

Atlantic

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

Australia

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

Brazil

Acre	DeNoronha	East	West

Canada

Atlantic	Central	East-Saskatchewan	Eastern
Mountain	Newfoundland	Pacific	Saskatchewan
Yukon			

Chile

Continental	EasterIsland

Etc

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

Europe

Amsterdam	Andorra	Athens	Belfast	Belgrade

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

GMT

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

Indian (Indian Ocean)

Antananarivo	Chagos	Christmas	Cocos	Comoro
Kerguelen	Mahe	Maldives	Mauritius	Mayotte
Reunion				

Mexico

BajaNorte	BajaSur	General

Miscellaneous

Arctic/ Longyearbyen	CET	CST6CDT	Cuba	EET

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

Pacific

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

US (United States)

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

Aliases

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