



EMC[®] Data Domain[®] Operating System

Version 5.6

Administration Guide

302-001-632

REV. 03

EMC²

Copyright © 2010-2016 EMC Corporation. All rights reserved. Published in the USA.

Published September 2016

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

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

EMC², EMC, and the EMC logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners.

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

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

CONTENTS

	Preface	13
Chapter 1	EMC Data Domain System Features and Integration	17
	Revision history.....	18
	EMC Data Domain system overview.....	18
	EMC Data Domain system features.....	19
	Data integrity.....	19
	Data compression.....	19
	Restore operations.....	20
	EMC Data Domain Replicator.....	20
	Multipath and load balancing.....	20
	System administrator access.....	20
	Licensed features.....	21
	Storage environment integration.....	22
Chapter 2	Getting Started	25
	DD System Manager overview.....	26
	Logging in and out of DD System Manager.....	26
	The DD System Manager interface.....	27
	Page elements.....	27
	Banner.....	28
	Navigation panel.....	28
	Information panel.....	28
	Help buttons.....	29
	Network Summary view.....	29
	Single system summary view.....	30
	End User License Agreement.....	30
	Selecting a system to manage.....	30
	Configuring the system with the configuration wizard.....	30
	License page.....	31
	Add License Key page.....	31
	Network General page.....	31
	Network Interfaces page.....	32
	Network DNS page.....	32
	System Settings Administrator page.....	33
	System Settings Email/Location page.....	34
	CIFS Protocol Authentication page.....	34
	CIFS Protocol Share page.....	34
	NFS Protocol Export page.....	35
	DD Boost Protocol Storage Unit page.....	35
	DD Boost Protocol Fibre Channel page.....	36
	VTL Protocol Library page.....	36
	VTL Protocol Access Group page.....	37
	Data Domain Command Line Interface.....	38
	Logging into the CLI.....	38
	CLI online help guidelines.....	39

Chapter 3	Managing Data Domain Systems	41
	System management overview.....	42
	System availability management.....	43
	Adding a system to DD System Manager.....	43
	Removing a system from DD System Manager.....	44
	Rebooting a system.....	44
	Powering a system on or off	44
	System upgrade management.....	45
	Viewing upgrade packages on the system.....	45
	Obtaining and verifying upgrade packages.....	46
	Upgrading a Data Domain system.....	47
	Removing an upgrade package.....	48
	Managing system licenses.....	48
	System storage management.....	49
	Viewing system storage information.....	49
	Physically locating a disk.....	53
	Configuring storage.....	53
	Network connection management.....	54
	Network interface management.....	54
	General network settings management.....	69
	Network route management.....	73
	System passphrase management.....	75
	Setting the system passphrase.....	75
	Changing the system passphrase.....	76
	System access management.....	77
	Role-based access control.....	77
	Access management for IP protocols.....	78
	Local user account management.....	86
	Directory user and group management.....	93
	Configuring mail server settings.....	101
	Managing time and date settings.....	101
	Managing system properties.....	102
	SNMP management.....	102
	Viewing SNMP status and configuration.....	103
	Enabling and disabling SNMP.....	104
	Downloading the SNMP MIB.....	104
	Configuring SNMP properties.....	105
	SNMP V3 user management.....	105
	SNMP V2C community management.....	107
	SNMP trap host management.....	109
	Autosupport report management.....	111
	Enabling and disabling autosupport reporting to EMC.....	111
	Reviewing generated autosupport reports.....	112
	Configuring the autosupport mailing list.....	112
	Support bundle management.....	113
	Generating a support bundle.....	113
	Viewing the support bundles list.....	114
	Alert notification management.....	114
	Viewing the notification group list.....	114
	Creating a notification group.....	116
	Managing the subscriber list for a group.....	116
	Modifying a notification group.....	117
	Deleting a notification group.....	117
	Resetting the notification group configuration.....	118
	Configuring the daily summary schedule and distribution list.....	118

	Enabling and disabling alert notification to EMC.....	119
	Testing the alerts email feature.....	120
	ConnectEMC management.....	120
	Viewing the ConnectEMC configuration, status, and history.....	121
	Setting and resetting the primary transport.....	121
	Adding and deleting alternate transports.....	121
	Configuring administrator notification.....	122
	Testing ConnectEMC operation.....	122
	Log file management.....	122
	Viewing log files in DD System Manager.....	123
	Displaying a log file in the CLI.....	124
	Learning more about log messages.....	124
	Saving a copy of log files.....	125
	Log message transmission to remote systems.....	126
	Remote system power management with IPMI.....	127
	IPMI and SOL limitations.....	128
	IPMI and SOL terminology.....	128
	Adding and deleting IPMI users with DD System Manager.....	129
	Changing an IPMI user password.....	130
	Configuring an IPMI port on a managed system.....	130
	Preparing for remote power management and console monitoring with the CLI.....	132
	Managing power with DD System Manager.....	133
	Managing power with the CLI.....	134
Chapter 4	Monitoring Data Domain Systems	135
	Viewing the summary status for all managed systems.....	136
	System Status area.....	136
	Space Usage area.....	137
	Systems area.....	137
	Viewing individual system status and identity information.....	137
	Alerts area.....	138
	File System area.....	138
	Services area.....	139
	Hardware area.....	139
	System area.....	139
	Alerts tab.....	140
	Viewing and clearing current alerts.....	140
	Current Alerts tab.....	141
	Viewing the alerts history.....	141
	Alerts History tab.....	142
	Viewing hardware component status.....	143
	Fan status.....	143
	Temperature status.....	144
	Power supply status.....	144
	PCI slot status.....	144
	NVRAM status.....	145
	Viewing system statistics.....	145
	Performance statistics graphs.....	146
	Viewing active users.....	147
	History report management.....	147
	Types of reports.....	148
	Creating a report.....	152
	Viewing saved reports.....	152
	Printing saved reports.....	153

	Deleting saved reports.....	153
	Renaming saved reports.....	153
	Viewing the Task Log.....	154
Chapter 5	File System	155
	File system overview.....	156
	How the file system stores data.....	156
	How the file system reports space usage.....	156
	How the file system uses compression	156
	How the file system implements data integrity.....	157
	How the file system reclaims storage space with file system cleaning	158
	Supported interfaces	159
	Supported backup software.....	159
	Data streams sent to a data domain system	159
	File system limitations.....	160
	Monitoring file system usage.....	162
	Accessing the file system view.....	162
	Managing file system operations.....	168
	Performing basic operations.....	169
	Performing cleaning.....	171
	Performing sanitization.....	172
	Modifying basic settings.....	174
	Fast copy operations.....	176
	Performing a fast copy operation.....	176
Chapter 6	MTrees	179
	MTrees overview.....	180
	Quotas.....	180
	About the MTree overview panel.....	181
	About the summary view.....	181
	About the space usage view (MTrees).....	184
	About the daily written view (MTrees).....	185
	Monitoring MTree usage.....	186
	Managing MTree operations.....	186
	Creating an MTree.....	186
	Configure and enable/disable MTree quotas.....	187
	Deleting an MTree.....	188
	Undeleting an MTree.....	189
	Renaming an MTree.....	189
	Replicating a system with quotas to one without.....	189
Chapter 7	Snapshots	191
	Snapshots overview.....	192
	Monitoring snapshots and their schedules.....	193
	About the snapshots view.....	193
	Managing snapshots.....	194
	Creating a snapshot.....	194
	Modifying a snapshot expiration date.....	195
	Renaming a snapshot.....	195
	Expiring a snapshot.....	195
	Managing snapshot schedules.....	196
	Creating a snapshot schedule.....	196

	Modifying a snapshot schedule.....	197
	Deleting a snapshot schedule.....	197
	Recover data from a snapshot.....	198
Chapter 8	CIFS	199
	CIFS overview.....	200
	Configuring SMB signing.....	200
	Performing CIFS setup.....	202
	Preparing clients for access to data domain systems.....	202
	Enabling CIFS services.....	202
	Naming the CIFS server.....	202
	Setting authentication parameters.....	203
	Disabling CIFS services.....	204
	Working with shares.....	204
	Creating shares on the Data Domain system.....	205
	Modifying a share on a Data Domain system.....	206
	Creating a share from an existing share.....	207
	Disabling a share on a Data Domain system.....	207
	Enabling a share on a Data Domain system.....	207
	Deleting a share on a Data Domain system.....	207
	Performing MMC administration.....	208
	Connecting to a Data Domain system from a CIFS client.....	208
	Displaying CIFS information.....	210
	Managing access control.....	210
	Accessing shares from a Windows client.....	210
	Providing domain users administrative access.....	210
	Allowing access from trusted domain users.....	210
	Allowing administrative access to a Data Domain system for domain users.....	211
	Restricting administrative access from Windows.....	211
	File access.....	211
	Monitoring CIFS operation.....	214
	Displaying CIFS status.....	214
	Display CIFS configuration.....	215
	Displaying CIFS statistics.....	217
	Performing CIFS troubleshooting.....	217
	Displaying clients current activity.....	217
	Setting the maximum open files on a connection.....	218
	Data Domain system clock.....	218
	Synchronizing from a Windows domain controller.....	218
	Synchronize from an NTP server.....	219
Chapter 9	NFS	221
	NFS overview.....	222
	Managing NFS client access to the Data Domain system.....	222
	Enabling NFS services.....	223
	Disabling NFS services.....	223
	Creating an export.....	223
	Modifying an export.....	225
	Creating an export from an existing export.....	226
	Deleting an export.....	226
	Displaying NFS information.....	226
	Viewing NFS status.....	227
	Viewing NFS exports.....	227

	Viewing active NFS clients.....	227
	Integrating a DDR into a Kerberos domain.....	228
	Add and delete KDC servers after initial configuration.....	229
Chapter 10	SCSI Target	233
	SCSI Target overview.....	234
	Working with physical resources.....	235
	Working with initiators.....	236
	Working with endpoints.....	238
	Fibre Channel view.....	242
	Physical Resources view.....	242
	Access Groups view.....	243
	Working with access groups.....	243
	Creating an access group.....	244
	Deleting an access group.....	244
	Working with a selected access group.....	245
	Adding an access group device.....	245
	Modifying or deleting an access group device.....	247
	Configuring the NDMP device TapeServer group.....	248
	Differences in FC link monitoring among DD OS versions.....	250
Chapter 11	Working with DD Boost	251
	About Data Domain Boost software.....	252
	Managing DD Boost with DD System Manager.....	252
	Specifying DD Boost user names.....	253
	Changing DD Boost user passwords.....	253
	Removing a DD Boost user name.....	254
	Enabling DD Boost.....	254
	Disabling DD Boost.....	254
	Viewing DD Boost storage units.....	254
	Creating a storage unit.....	255
	Viewing storage unit information.....	257
	Modifying a storage unit.....	259
	Renaming a storage unit.....	260
	Deleting a storage unit.....	260
	Undeleting a storage unit.....	260
	Selecting DD Boost options.....	261
	Managing certificates for DD Boost.....	262
	Managing DD Boost client access and encryption.....	264
	About interface groups.....	265
	Interfaces.....	266
	Clients.....	267
	Interface enforcement.....	267
	Creating interface groups.....	268
	Deleting an interface group.....	268
	Enabling and disabling interface groups.....	269
	Modifying an interface group's name and interfaces.....	269
	Deleting a client from the interface group.....	269
	Modifying a client's name or interface group.....	270
	Destroying DD Boost.....	270
	Configuring DD Boost-over-Fibre Channel.....	271
	Enabling DD Boost users.....	271
	Configuring DD Boost.....	272
	Verifying connectivity and creating access groups.....	273

	About the DD Boost tabs	275
	Settings	275
	Checking activities	275
	Checking interface groups and clients	276
	Checking storage units	277
Chapter 12	DD Virtual Tape Library	279
	DD Virtual Tape Library overview	280
	Planning a VTL	280
	VTL limits	281
	Number of drives supported by a VTL	282
	Tape barcodes	282
	LTO tape drive compatibility	283
	Setting up a VTL	284
	Managing a VTL	284
	Enabling VTL	286
	Disabling VTL	286
	Configuring VTL service options	287
	Working with libraries	287
	Creating libraries	288
	Deleting libraries	290
	Searching for tapes	290
	Working with a selected library	291
	Creating tapes	291
	Deleting tapes	292
	Importing tapes	293
	Exporting tapes	295
	Moving tapes between devices within a library	296
	Adding slots	297
	Deleting slots	297
	Adding CAPs	297
	Deleting CAPs	298
	Viewing changer information	298
	Working with drives	299
	Creating drives	300
	Deleting drives	300
	Working with a selected drive	301
	Working with tapes	301
	Changing a tape's write or retention lock state	302
	Working with the vault	303
	Working with pools	303
	Creating pools	304
	Working with a selected pool	305
	Converting a directory pool to an MTree pool	306
	Moving tapes between pools	306
	Copying tapes between pools	308
	Renaming pools	308
	Deleting pools	309
Chapter 13	DD Replicator	311
	DD Replicator overview	312
	Prerequisites for replication configuration	312
	Replication version compatibility	313
	Using DD Encryption with DD Replicator	316

	Replication types.....	316
	Managed file replication	317
	Directory replication.....	318
	MTree replication.....	319
	Collection replication	320
	Replication topologies.....	320
	One-to-one replication.....	322
	Bi-directional replication.....	322
	One-to-many replication.....	323
	Many-to-one replication.....	323
	Cascaded replication.....	324
	Managing replication.....	325
	Replication status.....	326
	Summary view.....	326
	DD Boost view.....	336
	Topology view.....	337
	Performance view.....	338
	Advanced Settings view.....	338
	Monitoring replication	341
	Checking replication pair status.....	341
	Viewing estimated completion time for backup jobs.....	341
	Checking replication context performance.....	341
	Tracking status of a replication process.....	341
Chapter 14	DD Secure Multitenancy	343
	Data Domain Secure Multitenancy overview.....	344
	Terminology used in SMT.....	344
	Data and control path isolation.....	345
	Understanding RBAC in Secure Multitenancy.....	345
	Provisioning a Tenant Unit.....	346
	Enabling Tenant Self-Service mode.....	346
	Data access by protocol.....	347
	Multi-User DD Boost and Storage Units in SMT.....	347
	Configuring access for CIFS.....	347
	Configuring NFS access.....	348
	Configuring access for VTL.....	348
	Using VTL NDMP TapeServer	349
	Data management operations.....	349
	Collecting performance statistics.....	349
	Modifying quotas.....	349
	SMT and replication.....	350
	SMT Tenant alerts.....	351
	Managing snapshots.....	351
	Performing a file system Fast Copy.....	351
Chapter 15	DD Extended Retention	353
	DD Extended Retention overview.....	354
	Supported protocols in DD Extended Retention.....	356
	Using DD Replicator with DD Extended Retention.....	356
	Collection replication with DD Extended Retention.....	356
	Directory replication with DD Extended Retention.....	356
	MTree replication with DD Extended Retention.....	357
	Managed file replication with DD Extended Retention.....	357
	Hardware and licensing for DD Extended Retention.....	357

	Hardware supported for DD Extended Retention	357
	Licensing for DD Extended Retention	360
	Adding shelf capacity licenses for DD Extended Retention	360
	Configuring storage for DD Extended Retention	360
	Customer-provided infrastructure for DD Extended Retention	361
	Managing DD Extended Retention	361
	Enabling DD systems for DD Extended Retention	361
	Creating a two-tiered file system for DD Extended Retention	362
	File system panel for DD Extended Retention	363
	File system tabs for DD Extended Retention	365
	Upgrades and recovery with DD Extended Retention	370
	Upgrading to DD OS 5.6 with DD Extended Retention	370
	Upgrading hardware with DD Extended Retention	371
	Recovering a DD Extended Retention-enabled system	371
Chapter 16	DD Retention Lock	373
	DD Retention Lock overview	374
	DD Retention Lock protocol	375
	DD Retention Lock flow	375
	Supported data access protocols	376
	Enabling DD Retention Lock on an MTree	377
	Enabling DD Retention Lock Governance on an MTree	377
	Enabling DD Retention Lock Compliance on an MTree	379
	Client-Side Retention Lock file control	380
	Setting Retention Locking on a file	381
	Extending Retention Locking on a file	383
	Identifying a Retention-Locked file	384
	Specifying a directory and touching only those files	384
	Reading a list of files and touching only those files	384
	Deleting or expiring a file	385
	Using ctime or mtime on Retention-Locked files	385
	System behavior with DD Retention Lock	385
	DD Retention Lock governance	385
	DD Retention Lock compliance	387
Chapter 17	DD Encryption	397
	DD encryption overview	398
	Configuring encryption	399
	About key management	400
	Rectifying lost or corrupted keys	400
	Key manager support	401
	Working with the RSA DPM Key Manager	401
	Working with the Embedded Key Manager	404
	How the cleaning operation works	404
	Key manager setup	405
	RSA DPM Key Manager encryption setup	405
	Changing key managers after setup	407
	Managing certificates for RSA Key Manager	408
	Checking settings for encryption of data at rest	409
	Enabling and disabling encryption of data at rest	409
	Enabling encryption of data at rest	409
	Disabling encryption of data at rest	409
	Locking and unlocking the file system	410
	Locking the file system	410

CONTENTS

Unlocking the file system 411
Changing the encryption algorithm 411

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 explains how to manage the EMC Data Domain® systems with an emphasis on procedures using the EMC Data Domain System Manager (DD System Manager), a browser-based graphical user interface (GUI). If an important administrative task is not supported in DD System Manager, the Command Line Interface (CLI) commands are described.

Note

- DD System Manager was formerly known as the Enterprise Manager.
- In some cases, a CLI command may offer more options than those offered by the corresponding DD System Manager feature. See the *EMC Data Domain Operating System Command Reference Guide* for a complete description of a command and its options.

Audience

This guide is for system administrators who are familiar with standard backup software packages and general backup administration.

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 Command Reference 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*

If you have the optional RSA Data Protection (DPM) Key Manager, see the latest version of the *RSA Data Protection Manager Server Administrator's Guide*, available with the RSA Key Manager product.

Special notice conventions used in this document

EMC uses the following conventions for special notices:

NOTICE

A notice identifies content that warns of a 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

EMC uses the following type style conventions in this document:

Table 1 Typography

Bold	Indicates interface element names, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)
<i>Italic</i>	Highlights publication titles listed in text
Monospace	Indicates system information, such as: <ul style="list-style-type: none"> • System code • System output, such as an error message or script • Pathnames, filenames, prompts, and syntax • Commands and options
<i>Monospace italic</i>	Highlights a variable name that must be replaced with a variable value
Monospace bold	Indicates text 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

The following topics describe how to get more product information and contact technical support.

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 (<https://support.emc.com>), and select 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 select the words. Then select ». In the list of categories under the Search box, select 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. Select 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.

CHAPTER 1

EMC Data Domain System Features and Integration

This chapter includes:

- [Revision history](#).....18
- [EMC Data Domain system overview](#)..... 18
- [EMC Data Domain system features](#)..... 19
- [Storage environment integration](#)..... 22

Revision history

The revision history lists the major changes to this document to support DD OS Release 5.6.

Table 2 Document revision history

Revision	Date	Description
03	September 2016	This revision includes minor updates.
02	June 2015	This revision includes minor updates.
01	April 2015	<p>This revision includes information about these new features:</p> <ul style="list-style-type: none"> • DD9500 equipment including DD9500 hardware supported for DD Extended Retention. • The Modify Password Policy dialog is renamed to Change Login Options. This dialog now features more password policy controls, as well as options to lock out a local user for a specified time after a sequence of unsuccessful login attempts. • The ConnectEMC feature is introduced to provide a secure alternative to sending alert and ASUP information in text form • The Capacity on Demand license is introduced to enable an on-demand capacity increase for DD2200 systems operating at the 4 TB storage level. <p>DD Boost changes:</p> <ul style="list-style-type: none"> • Mentioned DFC (DD Boost-over-Fibre Channel) support for the AIX client environment. • Added the section, "Managing Certificates for DD Boost."

EMC Data Domain system overview

EMC Data Domain systems are disk-based inline deduplication appliances and gateways that provide data protection and disaster recovery (DR) in the enterprise environment.

All systems run the EMC Data Domain Operating System (DD OS), which provides both a command-line interface (CLI) for performing all system operations, and the EMC Data Domain System Manager (DD System Manager) graphical user interface (GUI) for configuration, management, and monitoring.

Note

DD System Manager was formerly known as the Enterprise Manager.

Systems consist of appliances that vary in storage capacity and data throughput. Systems are typically configured with expansion shelves that add storage space.

Note

Legacy Data Domain Gateway systems store all data on qualified third-party storage arrays through a Fibre Channel interface. See the list of qualified arrays in the *Storage Array Compatibility List* at <https://support.emc.com>.

EMC Data Domain system features

Data Domain system features ensure data integrity, reliable restoration, efficient resource usage, and ease of management. Licensed features allow you to scale the system feature set to match your needs and budget.

Data integrity

The DD OS Data Invulnerability Architecture™ protects against data loss from hardware and software failures.

- When writing to disk, the DD OS creates and stores checksums and self-describing metadata for all data received. After writing the data to disk, the DD OS then recomputes and verifies the checksums and metadata.
- An append-only write policy guards against overwriting valid data.
- After a backup completes, a validation process examines what was written to disk and verifies that all file segments are logically correct within the file system and that the data is identical before and after writing to disk.
- In the background, the online verify operation continuously checks that data on the disks is correct and unchanged since the earlier validation process.
- Storage in most Data Domain systems is set up in a double parity RAID 6 configuration (two parity drives). Additionally, most configurations include a hot spare in each enclosure, except the DD1xx series systems, which use eight disks. Each parity stripe uses block checksums to ensure that data is correct. Checksums are constantly used during the online verify operation and while data is read from the Data Domain system. With double parity, the system can fix simultaneous errors on as many as two disks.
- To keep data synchronized during a hardware or power failure, the Data Domain system uses NVRAM (non-volatile RAM) to track outstanding I/O operations. An NVRAM card with fully charged batteries (the typical state) can retain data for a period of hours, which is determined by the hardware in use.
- When reading data back on a restore operation, the DD OS uses multiple layers of consistency checks to verify that restored data is correct.

Data compression

DD OS data compression identifies redundant data during each backup and stores unique data just once.

The storage of unique data is invisible to backup software and independent of data format. Data can be structured, such as databases, or unstructured, such as text files. Data can derive from file systems or from raw volumes.

Typical compression ratios are 20-to-1, on average, over many weeks. This ratio assumes there are weekly full backups and daily incremental backups. A backup that includes many duplicate or similar files (files copied several times with minor changes) benefits the most from compression.

Depending on backup volume, size, retention period, and rate of change, the amount of compression can vary. The best compression happens with backup volume sizes of at least 10 MiB (MiB is the base 2 equivalent of MB).

To take full advantage of multiple Data Domain systems, a site with more than one Data Domain system must consistently backup the same client system or set of data to the same Data Domain system. For example, if a full back up of all sales data goes to Data Domain system A, maximum compression is achieved when the incremental backups and future full backups for sales data also go to Data Domain system A.

Restore operations

File restore operations create little or no contention with backup or other restore operations.

When backing up to disks on a Data Domain system, incremental backups are always reliable and can be easily accessed. With tape backups, a restore operation may rely on multiple tapes holding incremental backups. Also, the more incremental backups a site stores on multiple tapes, the more time-consuming and risky the restore process. One bad tape can kill the restore.

Using a Data Domain system, you can perform full backups more frequently without the penalty of storing redundant data. Unlike tape drive backups, multiple processes can access a Data Domain system simultaneously. A Data Domain system allows your site to offer safe, user-driven, single-file restore operations.

EMC Data Domain Replicator

The EMC Data Domain Replicator sets up and manages the replication of backup data between two Data Domain systems.

A Replicator pair consists of a source and a destination system and replicates a complete data set, directory, or MTree from the source system to the destination system. An individual Data Domain system can be a part of multiple replication pairs and can serve as a source for one or more pairs and a destination for one or more pairs. After replication is started, the source system automatically sends any new backup data to the destination system.

Multipath and load balancing

A multipath condition is created when two or more paths are established between a Data Domain system and a backup server or backup destination array. When multiple paths are present, the system automatically balances the backup load between the available paths.

At least two HBA ports are required to create a multipath configuration. When connected to a backup server, each of the HBA ports on the multipath is connected to a separate port on the backup server. On a Data Domain gateway, each of the multipath HBA ports are connected to a separate port on the array that the gateway uses as a backup destination.

System administrator access

System administrators can access the system for configuration and management using a command line interface or a graphical user interface.

- **DD OS CLI**—A command-line interface that is available through a serial console or through Ethernet connections using SSH or Telnet. CLI commands enable initial system configuration, changes to individual system settings, and display of system operation status.

- **DD System Manager**—A browser-based graphical user interface that is available through Ethernet connections. Use DD System Manager to perform initial system configuration, make configuration changes after initial configuration, display system and component status, and generate reports and charts. DD System Manager also provides centralized management for multiple systems.

Note

Some older systems support access using a keyboard and monitor attached directly to the system.

Licensed features

Feature licenses allow you to purchase only those features you intend to use. Some examples of features that require licenses are Extended Retention, DD Boost, and storage capacity increases.

Consult with your EMC representative for information on purchasing licensed features.

Table 3 Features requiring licenses

Feature Name	License Name in Software	Description
EMC Data Domain ArchiveStore	ARCHIVESTORE	Licenses Data Domain systems for archive use, such as file and email archiving, file tiering, and content and database archiving.
EMC Data Domain Boost	DDBOOST	Enables the use of a Data Domain system with the following applications: EMC Avamar, EMC NetWorker, Oracle RMAN, Quest vRanger, Symantec Veritas NetBackup (NBU), and Backup Exec. The managed replication feature of DD Boost also requires the DD Replicator license.
EMC Data Domain Capacity on Demand	CONTROLLER-COD	Enables an on-demand capacity increase for 4 TB DD2200 systems to 7.5 TB or 13.18 TB. An increase to 13.18 TB also requires the EXPANDED-STORAGE license.
EMC Data Domain Encryption	ENCRYPTION	Allows data on system drives or external storage to be encrypted while being saved, and then locked before moving it to another location.
EMC Data Domain Expansion Storage	EXPANDED-STORAGE	Allows Data Domain system storage to be expanded beyond the level provided in the base system.
EMC Data Domain Extended Retention (formerly DD Archiver)	EXTENDED-RETENTION	Licenses the Extended Retention storage feature.
EMC Data Domain I/OS (for IBM i operating environments)	I/OS	An I/OS license is required when VTL is used to backup systems in the IBM i operating environment. Apply this license before adding virtual tape drives to libraries.
EMC Data Domain Replicator	REPLICATION	Adds DD Replicator for replication of data from one Data Domain system to another. A license is required on each system.

Table 3 Features requiring licenses (continued)

Feature Name	License Name in Software	Description
EMC Data Domain Retention Lock Compliance Edition	RETENTION-LOCK-COMPLIANCE	Meets the strictest data retention requirements from regulatory standards such as SEC17a-4.
EMC Data Domain Retention Lock Governance Edition	RETENTION-LOCK-GOVERNANCE	Protects selected files from modification and deletion before a specified retention period expires.
EMC Data Domain Shelf Capacity-Active Tier	CAPACITY-ACTIVE	Enables a Data Domain system to expand the active tier storage capacity to an additional shelf.
EMC Data Domain Shelf Capacity-Archive Tier	CAPACITY-ARCHIVE	Enables a Data Domain system to expand the archive tier storage capacity to an additional shelf.
EMC Data Domain Virtual Tape Library (VTL)	VTL	Enables the use of a Data Domain system as a virtual tape library over a Fibre Channel network. This license also enables the NDMP Tape Server feature, which previously required a separate license.
Gateway Expanded Storage Level 2	GATEWAY-EXPANDED-STORAGE-LEVEL-2	Enables gateway systems to support additional usable capacity.
Gateway Expanded Storage Level 3	GATEWAY-EXPANDED-STORAGE-LEVEL-3	Enables gateway systems to support additional capacity greater than Expanded Storage Level 2 usable capacity.

Storage environment integration

EMC Data Domain systems integrate easily into existing data centers.

- All Data Domain systems can be configured as storage destinations for leading backup and archiving applications using NFS, CIFS, Boost, or VTL protocols.
- Search for *compatibility documents* at <https://support.emc.com> for information on the applications that work with the different configurations.
- The Data Domain gateway series uses external disk arrays for storage. Data Domain gateways work with Data Domain arrays and are also qualified with storage systems from several leading enterprise storage providers.
- Multiple backup servers can share one Data Domain system.
- One Data Domain system can handle multiple simultaneous backup and restore operations.
- Multiple Data Domain systems can be connected to one or more backup servers.

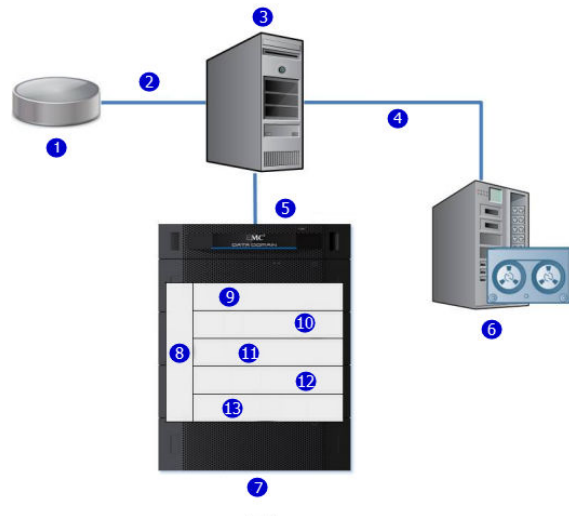
For use as a backup destination, a Data Domain system can be configured either as a disk storage unit with a file system that is accessed through an Ethernet connection or as a virtual tape library (VTL) that is accessed through a Fibre Channel connection. The VTL feature enables Data Domain systems to be integrated into environments where backup software is already configured for tape backups, minimizing disruption.

Configuration is performed both in the DD OS, as described in the relevant sections of this guide, and in the backup application, as described in the backup application's administrator guides and in Data Domain application-related guides and tech notes.

- All backup applications can access a Data Domain system as either an NFS or a CIFS file system on the Data Domain disk device.
- The following applications work with a Data Domain system using the DD Boost interface: EMC Avamar, EMC NetWorker, Oracle RMAN, Quest vRanger, Symantec Veritas NetBackup (NBU), and Backup Exec.

The following figure shows a Data Domain system integrated into an existing basic backup configuration.

Figure 1 Data Domain system integrated into a storage environment



1. Primary storage
2. Ethernet
3. Backup server
4. SCSI/Fibre Channel
5. Gigabit Ethernet or Fibre Channel
6. Tape system
7. Data Domain system
8. Management
9. NFS/CIFS/VTL/DD Boost
10. Data Verification
11. Data Domain file system
12. Global compression
13. RAID

As shown in Figure 1, data flows to a Data Domain system through an Ethernet or Fibre Channel connection. Immediately, the data verification processes begin and are continued while the data resides on the Data Domain system. In the file system, the DD OS Global Compression™ algorithms dedupe and compress the data for storage. Data is then sent to the disk RAID subsystem. When a restore operation is required, data is retrieved from Data Domain storage, decompressed, verified for consistency, and transferred via Ethernet to the backup servers using Ethernet (for NFS, CIFS, DD Boost), or using Fiber Channel (for VTL and DD Boost).

The DD OS accommodates relatively large streams of sequential data from backup software and is optimized for high throughput, continuous data verification, and high

compression. It also accommodates the large numbers of smaller files in nearline storage (DD ArchiveStore).

Data Domain system performance is best when storing data from applications that are not specifically backup software under the following circumstances.

- Data is sent to the Data Domain system as sequential writes (no overwrites).
- Data is neither compressed nor encrypted before being sent to the Data Domain system.

CHAPTER 2

Getting Started

This chapter includes:

- [DD System Manager overview](#)26
- [Logging in and out of DD System Manager](#) 26
- [The DD System Manager interface](#) 27
- [Selecting a system to manage](#) 30
- [Configuring the system with the configuration wizard](#) 30
- [Data Domain Command Line Interface](#) 38
- [Logging into the CLI](#) 38
- [CLI online help guidelines](#) 39

DD System Manager overview

DD System Manager is a browser-based graphical user interface, available through Ethernet connections, for managing up to 20 systems (depending on the model) at any location. DD System Manager provides a single, consolidated management interface that allows for configuration and monitoring of many system features and system settings.

DD System Manager provides real-time graphs and tables that allow you to monitor the status of system hardware components and configured features.

Additionally, a command set that performs all system functions is available to users at the command-line interface (CLI). Commands configure system settings and provide displays of system hardware status, feature configuration, and operation.

The command-line interface is available through a serial console or through an Ethernet connection using SSH or Telnet.

Note

Some older systems support access using a keyboard and monitor attached directly to the system.

Logging in and out of DD System Manager

Use a browser to log in to DD System Manager.

Procedure

1. Open a web browser and enter the IP address or hostname to connect to DD System Manager. It must be:
 - A fully qualified domain name (for example, `http://dd01.emc.com`)
 - A hostname (`http://dd01`)
 - An IP address (`http://10.5.50.5`)

Note

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

2. For HTTPS secure login, click **Secure Login**.

Secure login with HTTPS requires a digital certificate to validate the identity of the DD OS system and to support bidirectional encryption between DD System Manager and a browser. DD OS includes a self-signed certificate, and DD OS allows you to import your own certificate.

The default settings of most browsers do not automatically accept a self-signed certificate. This does not prevent you from using the self-signed certificate; it just means that you must respond to a warning message each time you perform a secure log in, or you must install the certificate in your browser. For instructions on how to install the certificate in your browser, see your browser documentation.

3. Enter your assigned username and password.

Note

The initial username is *sysadmin* and the initial password is the system serial number. For information on setting up a new system, see the *EMC Data Domain Operating System Initial Configuration Guide*.

4. Click **Log In**.

The Summary view appears in the Information panel.

Note

If you enter an incorrect password 4 consecutive times, the system locks out the specified username for 120 seconds. The login count and lockout period are configurable and might be different on your system.

5. To log out, click **Log Out** in the DD System Manager banner.

When you log out, the system displays the log in page with a message that your log out is complete.

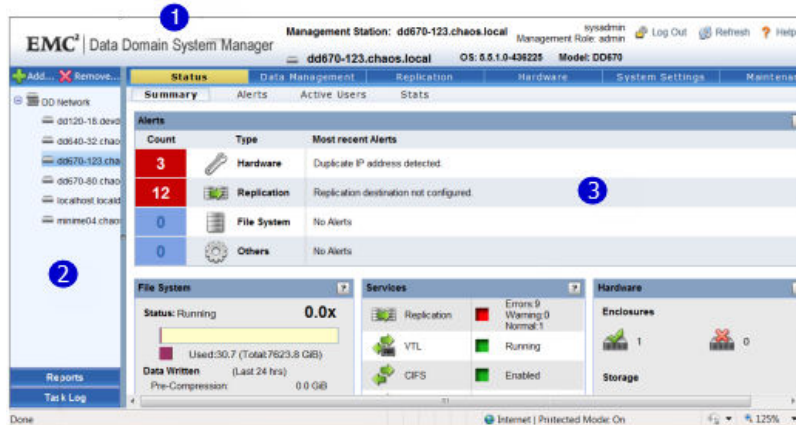
The DD System Manager interface

The DD System Manager interface provides common elements on most pages that enable you to quickly identify the managed system, get context sensitive help, and navigate through the management options.

Page elements

The primary page elements are the banner, Navigation panel, and Information panel.

Figure 2 DD System Manager page components



1. Banner
2. Navigation panel
3. Information panel

Banner

The DD System Manager banner displays important information about the management station and the managed stations, and it displays information and controls for the current management session.

The banner lists the following information and controls.

- Management station hostname.
- Selected system hostname.
- DD OS version
- Selected system model number.
- User name and role for the current logged in user.
- **Log Out** icon. Click to log out of the current session.
- **Refresh** icon. Click to refresh the DD System Manager display.
- **Help** icon. Click to view the top-level online help.

Navigation panel

The Navigation panel displays the managed systems and allows you to select a summary view, add or delete managed systems, or select a system to manage. Additional controls provide access to the Reports and Task Log features.

You can use the Navigation panel to initiate the following tasks.

- Click the **Add** or **Remove** icons to add or remove a system managed by the DD System Manager.
- Click the top-level **DD Network** icon to display the DD Network Summary view.
- Click **+** or **-** to the left of DD Network to display or hide the systems that DD System Manager is managing.
- Expand the DD Network and select a system in the tree to display the Single System Summary view, where tabs allow you to configure and monitor the selected system.
- Click **Reports** to open a report generator tool and provide access to saved reports for the selected system. Reports for file system and replication usage statistics can be generated.
- Click **Task Log** to show a history of tasks that were previously performed on the system you are logged into.

Information panel

The Information panel displays information and controls related to the selected item in the Navigation panel (either the DD Network or a managed system). The information panel is where you find system status information and configure a system.

Depending on the feature you have selected, the Information panel displays one or more tab bars, table view controls, and the More Tasks menu.

Tab bar

When you select a single system in the Navigation panel, the Tab bar appears. Its tabs provide access to the configuration and monitoring tools for the system. Many of these tabs display their own set of tabs. The top-level set of tabs are as follows:

- **Status**—displays important information about the system. Subtabs include Summary, Alerts, Active Users, and Stats.

- **Data Management**—contains subtabs for File System, MTree, Quota, Snapshots, CIFS, NFS, VTL, and DD Boost.
- **Replication**—provides data replication monitoring and management tools.
- **Hardware**—provides tabs for monitoring health and statistics of hardware for Storage, Network, Fibre Channel, and Chassis.
- **System Settings**—provides tabs for Licenses, Access Management, and General Configuration.
- **Maintenance**—provides tabs for System, Support, Logs, and IPMI.

Working with table view options

Many of the views with tables of items contain controls for filtering, navigating, and sorting the information in the table.

How to use common table controls:

- Click the diamond icon in a column heading to reverse the sort order of items in the column.
- Click the ◀ and ▶ arrows at the bottom right of the view to move forward or backward through the pages. To skip to the beginning of a sequence of pages, click ◀◀. To skip to the end, click ▶▶.
- Use the scroll bar to view all items in a table.
- Enter text in the **Filter By** box to search for or prioritize the listing of those items.
- Click **Update** to refresh the list.
- Click **Reset** to return to the default listing.

More Tasks menu

Some pages provide a More Tasks menu at the top of the view that contains commands related to the current view.

Help buttons

Help buttons display a ? and appear in the banner, in the title of many areas of the Information panel, and in many dialogs. Click the help button to display a help window related to the current feature you are using.

The help window provides a contents button and navigation button above the help. Click the contents button to display the guide contents and a search button that you can use to search the help. Use the directional arrow buttons to page through the help topics in sequential order.

Network Summary view

The network Summary view presents a status report for all systems managed by DD System Manager and summarizes key operating information.

To select the network Summary view, click DD Network in the Navigation panel. If you select any managed system, the view will change to the summary view for that managed system.

The network Summary view appears in the Information panel. A tally of alerts and charts of disk space enable you to identify problems. Click on a system in the Systems list to display the summary view for that system. Click an item in the Status column to learn more information about an alert or error.

Single system summary view

The single system summary view presents a status report for a single system and summarizes key operating information.

To display summary information about a single system, select the system in the Navigation panel, and then select **Status** > **Summary** in the Information panel. This view displays important data about the selected system and displays a set of tabs at the top of the Information panel. You can use these tabs to configure and monitor the selected system. Click on any item in the Summary view to display a tab with more information for that item.

End User License Agreement

To view the End User License Agreement (EULA), select **Maintenance** > **More Tasks** > **EULA**.

Selecting a system to manage

DD System Manager is designed to manage multiple systems. The network summary view is the default view at startup and displays information for all managed systems. To display information for a specific system, you must select that system.

Procedure

1. In no systems are listed in the Navigation panel, click the DD Network + button (not the + button at the top of the panel) to display a list of managed systems.

The management system is always listed. Additional managed systems must be added before they can appear in the list.

2. Select a system in the Navigation panel.

The Information panel displays information unique to the selected system.

Configuring the system with the configuration wizard

There are two wizards, a DD System Manager configuration wizard and a Command Line Interface (CLI) configuration wizard. The configuration wizards guide you through a simplified configuration of your system to get your system operating quickly.

After you complete the basic configuration with a wizard, you can use additional configuration controls in DD System Manager and the CLI to further configure your system.

Note

The following procedure describes how to start and run the DD System Manager configuration wizard after the initial configuration of your system. For instructions on running the configuration wizards at system startup, see the *EMC Data Domain Operating System Initial Configuration Guide*.

Procedure

1. Select a system in the Navigation panel.
2. Select **Maintenance** > **System**.
3. Select **More Tasks** > **Launch Configuration Wizard**.

- Use the controls at the bottom of the Configuration Wizard dialog to select which features you want to configure and to advance through the wizard. To display help for a feature, click the help icon (question mark) in the lower left corner of the dialog.

License page

The License page displays all installed licenses. Click **Yes** to add a license or click **No** to skip license installation.

Add License Key page

The Add License Key page accepts a single license per line. Press Enter after you enter each license key, and click **Add** when you are done.

Network General page

The General page allows you to configure network settings that define how the system participates in an IP network.

To configure these network settings outside of the configuration wizard, select **Hardware > Network**.

Table 4 General page settings

Item	Description
Obtain Settings using DHCP	Select this option to specify that the system collect network settings from a Dynamic Host Control Protocol (DHCP) server. When you configure the network interfaces, at least one of the interfaces must be configured to use DHCP.
Manually Configure	Select this option to use the network settings defined in the Settings area of this page.
Host Name	Specifies the network hostname for this system.
<p>Note</p> <p>If you choose to obtain the network settings through DHCP, you can manually configure the hostname at Hardware > Network > Settings or with the <code>net set hostname</code> command. You must manually configure the host name when using DHCP over IPv6.</p>	
Domain Name	Specifies the network domain to which this system belongs.
Default IPv4 Gateway	Specifies the IPv4 address of the gateway to which the system will forward network requests when there is no route entry for the destination system.
Default IPv6 Gateway	Specifies the IPv6 address of the gateway to which the system will forward network requests when there is no route entry for the destination system.

Network Interfaces page

The Interfaces page allows you to configure network settings that define how each interface participates in an IP network.

To Configure these network settings outside of the configuration wizard, select **Hardware** › **Network**.

Table 5 Interfaces page settings

Item	Description
Interface	Lists the interfaces available on your system.
Enabled	Shows whether each interface is enabled (checkbox selected) or disabled (not selected). Click the checkbox to toggle the interface between the enabled and disabled states.
DHCP	Shows the current Dynamic Host Control Protocol (DHCP) configuration for each interface. Select v4 for IPv4 DHCP connections, v6 for IPv6 connections, or no to disable DHCP.
IP Address	Specifies an IPv4 or IPv6 address for this system. To configure the IP address, you must set DHCP to No .
	<p>Note</p> <p>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.</p>
Netmask	Specifies the network mask for this system. To configure the network mask, you must set DHCP to No .
Link	Displays whether the Ethernet connection is active (Yes) or not (No).

Network DNS page

The DNS page allows you to configure how the system obtains IP addresses for DNS servers in a Domain Name System (DNS).

To Configure these network settings outside of the configuration wizard, select **Hardware** › **Network**.

Table 6 DNS page settings

Item	Description
Obtain Settings using DHCP.	Select this option to specify that the system collect DNS IP addresses from a Dynamic Host Control Protocol (DHCP) server. When you configure the network interfaces, at least one of the interfaces must be configured to use DHCP.
Manually configure DNS list.	Select this option when you want to manually enter DNS server IP addresses.

Table 6 DNS page settings (continued)

Item	Description
Add (+) button	Click this button to display a dialog in which you can add a DNS IP address to the DNS IP Address list. You must select Manually configure DNS list before you can add or delete DNS IP addresses.
Delete (X) button	Click this button to delete a DNS IP address from the DNS IP Address list. You must select the IP address to delete before this button is enabled. You must also select Manually configure DNS list before you can add or delete DNS IP addresses.
IP Address Checkboxes	Select a checkbox for a DNS IP address that you want to delete. Select the DNS IP Address checkbox when you want to delete all IP addresses. You must select Manually configure DNS list before you can add or delete DNS IP addresses.

System Settings Administrator page

The Administrator page allows you to configure the administrator password and how the system communicates with the administrator.

To Configure these settings outside of the configuration wizard, select **System Settings > Access Management > Local Users**.

Table 7 Administrator page settings

Item	Description
User Name	The default administrator name is <i>sysadmin</i> . The sysadmin user cannot be renamed or deleted. You can create other users (including other administrators) by selecting System Settings > Access Management > Local Users .
Password	Type the password for sysadmin.
Verify Password	Retype the password for sysadmin.
Admin Email	Specify the email address to which DD System Manager sends alert and autosupport email messages.
Send Alert Notification Emails to this address	Check to configure DD System Manager to send alert notifications to sysadmin as alert events occur. To manage alert notification outside of this wizard, select Status > Alerts > Notification .
Send Daily Alert Summary Emails to this address	Check to configure DD System Manager to send alert summaries to sysadmin at the end of each day.
Send Autosupport Emails to this address	Check to configure DD System Manager to send the sysadmin user autosupport emails, which are daily reports that document system activity and status. To manage autosupport notification outside of this wizard, select Maintenance > Support > Autosupport .

System Settings Email/Location page

The Email/Location page allows you to configure the mail server name, control what system information is sent to Data Domain, and specify a location name to identify your system.

Table 8 Email/Location page settings

Item	Description
Mail Server	Specify the name of the mail server that manages emails to and from the system.
Send Alert Notification Emails to Data Domain	Check to configure DD System Manager to send alert notification emails to Data Domain. To manage alert notification outside of this wizard, select Status > Alerts > Notification .
Send Vendor Support Notification Emails to Data Domain	Check to configure DD System Manager to send vendor support notification emails to Data Domain.
Location	Use this optional attribute as needed to record the location of your system. If you specify a location, this information is stored as the SNMP system location.

CIFS Protocol Authentication page

The Authentication page enables you to configure Active Directory, Workgroup and NIS authentication information for your system.

To configure these settings outside of the configuration wizard, select **System Settings > Access Management > Authentication**.

Table 9 Authentication page settings

Item	Description
Active Directory/Kerberos Authentication	Expand this panel to enable, disable, and configure Active Directory Kerberos authentication.
Workgroup Authentication	Expand this panel to configure Workgroup authentication.
NIS Authentication	Expand this panel to enable, disable, and configure NIS authentication, servers, and groups.

CIFS Protocol Share page

The Share page enables you to configure a CIFS protocol share name and a directory path for your system.

To configure these settings outside of the configuration wizard, select **Data Management > CIFS**.

Table 10 Share page settings

Item	Description
Share Name	Enter a share name for the system.
Directory Path	Enter a directory path for the system.
Add (+) button	Click + to enter a system client.
Delete (X) button	Click X to delete a selected client.

NFS Protocol Export page

The Export page enables you to configure an NFS protocol export directory path and network clients.

To configure these settings outside of the configuration wizard, select **Data Management > NFS**.

Table 11 Export page settings

Item	Description
Directory Path	Enter a pathname for the export.
Add (+) button	Click + to enter a system client.
Delete (X) button	Click X to delete a selected client.

DD Boost Protocol Storage Unit page

The Storage Unit page allows you to configure DD Boost storage units.

To configure these settings outside of the configuration wizard, select **Data Management > DD Boost > Storage Units > + (plus sign)** to add a storage unit, **the pencil** to modify a storage unit, or **X** to delete a storage unit.

Table 12 Storage Unit page settings

Item	Description
Storage Unit	The name of your DD Boost Storage Unit. You may optionally change this name.
User	For the default DD Boost user, either select an existing user, or select Create a new Local User, and enter their User name, Password, and Management Role. This role can be one of the following: <ul style="list-style-type: none"> <i>Admin role:</i> Lets you configure and monitor the entire Data Domain system. <i>User role:</i> Lets you monitor Data Domain systems and change your own password. <i>Security role:</i> In addition to user role privileges, lets you set up security-officer configurations and manage other security-officer operators.

Table 12 Storage Unit page settings (continued)

Item	Description
	<ul style="list-style-type: none"> <i>Backup-operator role:</i> In addition to user role privileges, lets you create snapshots, import and export tapes to a VTL, and move tapes within a VTL. <i>None role:</i> Intended only for EMC DD Boost authentication, so you cannot monitor or configure a Data Domain system.

DD Boost Protocol Fibre Channel page

The Fibre Channel page allows you to configure DD Boost Access Groups over Fibre Channel.

To configure these settings outside of the configuration wizard, select **Data Management** › **DD Boost** › **Fibre Channel** › **+** (plus sign) to add an access group, the **pencil** to modify an access group, or **X** to delete an access group.

Table 13 Fibre Channel page settings

Item	Description
Configure DD Boost over Fibre Channel	Select the checkbox if you want to configure DD Boost over Fibre Channel.
Group Name (1-128 Chars)	Create an Access Group. Enter a unique name. Duplicate access groups are not supported.
Initiators	Select one or more initiators. Optionally, replace the initiator name by entering a new one. An initiator is a backup client that connects to the system to read and write data using the FC (Fibre Channel) protocol. A specific initiator can support DD Boost over FC or VTL, but not both.
Devices	The devices to be used are listed. They are available on all endpoints. An endpoint is the logical target on the Data Domain system to which the initiator connects.

VTL Protocol Library page

The Library page allows you to configure VTL protocol settings for a library.

To configure these settings outside of the configuration wizard, select **Data Management** › **VTL** › **Virtual Tape Libraries** › **VTL Service** › **Libraries** › **More Tasks** › **Library** › **Create**

Table 14 Library page settings

Item	Description
Library Name	Enter a name of from 1 to 32 alphanumeric characters.
Number of Drives	Number of supported tape drives.
Drive Model	Select the desired model from the drop-down list: <ul style="list-style-type: none"> IBM-LTO-1

Table 14 Library page settings (continued)

Item	Description
	<ul style="list-style-type: none"> • IBM-LTO-2 • IBM-LTO-3 • IBM-LTO-4 • IBM-LTO-5 (default) • HP-LTO-3 • HP-LTO-4
Number of Slots	Enter the number of slots per library: <ul style="list-style-type: none"> • Up to 32,000 slots per library • Up to 64,000 slots per system • This should be equal to, or greater than, the number of drives.
Number of CAPs	(Optional) Enter the number of cartridge access ports (CAPs): <ul style="list-style-type: none"> • Up to 100 CAPs per library • Up to 1000 CAPs per system
Changer Model Name	Select the desired model from the drop-down list: <ul style="list-style-type: none"> • L180 (default) • RESTORER-L180 • TS3500 • I2000 • I6000 • DDVTL
Starting Barcode	Enter the desired barcode for the first tape, in the format A990000LA.
Tape Capacity	(Optional) Enter the tape capacity. If not specified, the capacity is derived from the last character of the barcode.

VTL Protocol Access Group page

The Access Group page allows you to configure VTL protocol settings for an access group. To configure these settings outside of the configuration wizard, select **Data Management** › **VTL** › **Access Groups** › **Groups** › **More Tasks** › **Group** › **Create**.

Table 15 Access Group page settings

Item	Description
Group Name	Enter a unique name of from 1 - 128 characters. Duplicate access groups are not supported.
Initiators	Select one or more initiators. Optionally, replace the initiator name by entering a new one. An initiator is a backup client that connects to a system

Table 15 Access Group page settings (continued)

Item	Description
	to read and write data using the Fibre Channel (FC) protocol. A specific initiator can support EMC DD Boost over FC or VTL, but not both.
Devices	The devices (drives and changer) to be used are listed. These are available on all endpoints. An endpoint is the logical target on the Data Domain system to which the initiator connects.

Data Domain Command Line Interface

The Command Line Interface (CLI) is a text driven interface that can be used instead of or in addition to DD System Manager. Most management tasks can be performed in DD System Manager or with the CLI. In some cases, the CLI offers configuration options and reports that are not yet supported in DD System Manager.

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

The Tab key can be used to do the following.

- Complete a command entry when that entry is unique. Tab completion is supported for all keywords. For example, entering `sys` Tab `sh` Tab `st` Tab displays the command `system show stats`.
- Show the next available option, if you do not enter any characters before pressing the Tab key.
- Show partial matched tokens or complete a unique entry, if you enter characters before pressing the Tab key.

The *EMC Data Domain Operating System Command Reference Guide* provides information for each of the CLI commands. Online help is available and provides the complete syntax for each command.

Logging into the CLI

You can access the CLI using a direct connection to the system or using an Ethernet connection through SSH or Telenet.

Before you begin

To use the CLI, you must establish a local or remote connection to the system using one of the following methods.

- If you are connecting through a serial console port on the system, connect a terminal console to the port and use the communication settings: 9600 baud, 8 data bits, no parity, and 1 stop bit.
- If the system provides keyboard and monitor ports, connect a keyboard and monitor to those ports.
- If you are connecting through Ethernet, connect a computer with SSH or Telnet client software to an Ethernet network that can communicate with the system.

Procedure

1. If you are using an SSH or Telnet connection to access the CLI, start the SSH or Telnet client and specify the IP address or host name of the system.

For information on initiating the connection, see the documentation for the client software. The system prompts you for your username.

2. When prompted, enter your system username.
3. When prompted, enter your system password.

The following example shows SSH login to a system named *mysystem* using SSH client software.

```
# ssh -l sysadmin mysystem.mydomain.com
Data Domain OS 5.6.0.0-19899
Password:
```

CLI online help guidelines

The CLI displays two types of help, syntax-only help and command-description help that includes the command syntax. Both types of help offer features that allow you reduce the time it takes to find the information you need.

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 3

Managing Data Domain Systems

This chapter includes:

- [System management overview](#)..... 42
- [System availability management](#)..... 43
- [System upgrade management](#)..... 45
- [Managing system licenses](#)..... 48
- [System storage management](#)..... 49
- [Network connection management](#)..... 54
- [System passphrase management](#)..... 75
- [System access management](#)..... 77
- [Configuring mail server settings](#)..... 101
- [Managing time and date settings](#)..... 101
- [Managing system properties](#)..... 102
- [SNMP management](#)..... 102
- [Autosupport report management](#)..... 111
- [Support bundle management](#)..... 113
- [Alert notification management](#)..... 114
- [ConnectEMC management](#)..... 120
- [Log file management](#)..... 122
- [Remote system power management with IPMI](#)..... 127

System management overview

DD System Manager allows you to manage the system on which DD System Manager is installed, and you can manage other systems as well. When DD System Manager manages other systems, the managing system is called a *management system*. A system that can be managed by DD System Manager on another system is called a *managed system*.

DD System Manager lists all managed systems in the Navigation panel. When you are working with a management system and one or more managed systems, consider the following guidelines.

- DD System Manager supports the management of systems running the previous version, the current version, and the next version when it becomes available. For Release 5.5, DD System Manager supports management of versions 5.4 to 5.6.
- To support replication, DD System Manager supports the addition of systems running the previous two versions, the current version and the next two versions as they become available. For Release 5.5, DD System Manager supports the addition of systems for replication for DD OS Version 5.2 to 5.6.
- The management system should be running the same DD OS version or a newer version than the managed systems. If a management system runs an older version of DD OS than what is on a managed system, the management station might not display all the features of the newer DD OS version.
- A managed system should be managed by one management system at one time.
- If you are an admin on the management system you become a global admin, which means that you can configure and monitor all managed systems.
- If you are a user on the management system you become a global user, which means that you can monitor all managed systems.

Note

When processing a heavy load, a system might be less responsive than normal. In this case, management commands issued from either DD System Manager or the CLI might take longer to complete. When the duration exceeds allowed limits, a timeout error is returned, even if the operation completed.

The following table recommends the maximum number of systems and user sessions that can be managed by DD System Manager:

Table 16 Maximum number of systems and users managed by DD System Manager

System Model	Maximum Active Users	Maximum Logged In Users	Maximum Systems
4 GB models ^a	5	10	8
8 GB models ^b	10	15	12
16 GB and greater models ^c	10	20	20

a. Includes DD140

b. Includes DD610 and DD630

c. Includes DD670, DD690, DD860, DD880, DD890, and DD990

System availability management

System availability management features allow you to select which systems to manage and how to reboot and manage power on those systems.

Adding a system to DD System Manager

Add systems to DD System Manager when you want to be able to manage multiple systems from the same DD System Manager session.

Note

Make sure the system being added is running a DD OS version that is compatible with the DD System Manager.

Procedure

1. Click the Add icon (+) on the Navigation panel.
2. In the Add System dialog box, enter the hostname or IP address of the system to be added in the System Name box.

Note

Do not add the same managed system to more than one instance of DD System Manager.

3. In Administration Credentials, enter the sysadmin user name in the **User Name** box, followed by the password.
4. Optionally, click **Advanced** to enter a proxy IP address (or system name) of a system that cannot be reached directly. If configured, enter a custom port instead of the default port 3009.

Note

IPv6 addresses are supported only when adding a DD OS 5.5 or later system to a management system using DD OS 5.5 or later.

5. Click **OK**.

Note

If the system is unreachable after adding it to DD System Manager, ensure there is a route from the managing system to the system being added. If a hostname (either a fully-qualified domain name (FQDN) or non-FQDN) is entered, make sure it is resolvable on the managed system. Configure a domain name for the managed system, ensure a DNS entry for the system exists, or ensure an IP address to hostname mapping is defined.

6. If the system certificate is not verified, the Verify Certificate dialog box shows details about the certificate. Check the system credentials. Click **OK** if you trust the certificate, or click **Cancel**.

Removing a system from DD System Manager

Remove a system from DD System Manager to make room to manage another system or when you no longer want to manage the managed system from the management system. You cannot remove the management system that hosts DD System Manager from DD System Manager.

Note

Removing a system removes it from the DD Network list. It does not delete any replication context configured to or from that system.

Procedure

1. Click the **X** (remove) icon on the Navigation panel.
2. In the Remove System(s) dialog box:
 - To remove all systems, select **System**.
 - To remove one or more systems, select the system.
3. Click **OK**.

Note

If only the DD System Manager host system is present, clicking the X icon results in a message stating that no removable systems are found on DD System Manager.

Rebooting a system

Reboot a system when a configuration change, such as changing the time zone, requires that you reboot the system.

Procedure

1. Select a system in the Navigation panel.
2. Select **Maintenance** > **System**.
3. From the More Tasks menu, select **Reboot System**.
4. Click **OK** to confirm.

Powering a system on or off

When powering a system off and on, it is important that you follow the proper procedure to preserve the file system and configuration integrity.

Procedure

1. Power on any expansion shelves before powering on the Data Domain controller. The ES30 powers on when plugged in. Wait approximately three minutes after all expansion shelves are turned on.

Note

The controller is the chassis and any internal storage. A *Data Domain system* refers to the controller and any optional external storage.

2. Plug in the power cord for your controller, and if there is a power button on the controller, press the power button (as shown in the *Installation and Setup Guide* for your Data Domain system).
3. To shut down power to a Data Domain system, use the `system poweroff` CLI command.

This command automatically performs an orderly shut down of DD OS processes and is available to administrative users only.

Results

NOTICE

Do not use the chassis power switch to power off the system. Doing so prevents remote power control using IPMI. Use the `system poweroff` command instead. The `system poweroff` command shuts down the system and turns off the power.

Note

The IMPI Remote System Power Down feature does not perform an orderly shutdown of the DD OS. Use this feature only if the `system poweroff` command is unsuccessful.

System upgrade management

To upgrade a DD OS system, you must verify that there is sufficient room for the new software on the target system, transfer the software to the system to be upgraded, and then start the upgrade.

Viewing upgrade packages on the system

DD System Manager allows you to view and manage up to five upgrade packages on a system. Before you can upgrade a system, you must download an upgrade package from the EMC Online Support site to a local computer, and then upload it to the target system.

Procedure

1. Expand **DD Network** in the Navigation panel, and select the system you want to manage.
2. Select **Maintenance** › **System**.

Results

For every package stored on the system, DD System Manager displays the filename, file size, and last modified date in the list titled: Upgrade Packages Available on Data Domain System.

Obtaining and verifying upgrade packages

You can use DD System Manager to locate upgrade package files on the Data Domain Support Web site and upload copies of those files to a system.

Note

You can use FTP or NFS to copy an upgrade package to a system. DD System Manager is limited to managing 5 system upgrade packages, but there are no restrictions, other than space limitations, when you manage the files directly in the `/ddvar/releases` directory. FTP is disabled by default. To use NFS, `/ddvar` needs to be exported and mounted from an external host).

Procedure

1. Expand **DD Network** in the Navigation panel, and select the system you want to upgrade.
2. Select **Maintenance > System**.
3. To obtain an upgrade package, click the **EMC Online Support** link, click Downloads, and use the search function to locate the package recommended for your system by Support personnel. Save the upgrade package to the local computer.
4. Verify that there are no more than four packages listed in the Upgrade Packages Available on Data Domain System list.

DD System Manager can manage up to five upgrade packages. If five packages appear in the list, remove at least one package before uploading the new package.

5. Click **Upload Upgrade Package** to initiate the transfer of the upgrade package to the target system.
6. In the Upload Upgrade Package dialog, click **Browse** to open the Choose File to Upload dialog. Navigate to the folder with the downloaded file, select the file, and click **Open**.
7. Click **OK**.

An upload progress dialog appears. Upon successful completion of the upload, the download file (with a `.rpm` extension) appears in the list titled: Upgrade Packages Available on Data Domain System.

8. To manually initiate an upgrade precheck, click **Upgrade Precheck**.

Note

The **Upgrade Precheck** button does not appear in releases prior to DD OS 5.5. If you are upgrading from a prior release, such as 5.4, this button does not appear until after you complete the upgrade to DD OS 5.5.

9. To verify the upgrade package integrity, click **View Checksum** and compare the calculated checksum displayed in the dialog to the authoritative checksum on the EMC Online Support site.

Note

The **View Checksum** button does not appear in releases prior to DD OS 5.5. If you are upgrading from a prior release, such as 5.4, this button does not appear until after you complete the upgrade to DD OS 5.5.

Upgrading a Data Domain system

When an upgrade file is present on a system, you can use DD System Manager to perform an upgrade using that file.

Note

System upgrade files use the .rpm file extension. This topic assumes that you are updating only DD OS. If you make hardware changes, such as adding, swapping, or moving interface cards, you must update the DD OS configuration to correspond with the hardware changes.

Procedure

1. After reading the Release Notes for instructions for this DD OS upgrade, log into the system where the upgrade is to be performed.
-

Note

For most releases, upgrades are permitted from up to two prior major release versions. For Release 5.5, upgrades are permitted from Releases 5.2, 5.3, and 5.4. Enhanced pre-upgrade checks are added in Release 5.5 and are not performed when upgrading from a Release 5.2 system.

Note

You cannot select a system from the DD Network list while logged in on another system.

2. Select **Data Management** > **File System**, and verify that the file system is enabled and running.
 3. Select **Maintenance** > **System**.
 4. From the Upgrade Packages Available on Data Domain System list, select the package to use for the upgrade.
-

Note

You must select an upgrade package for a newer version of DD OS. DD OS does not support downgrades to previous versions.

5. Click **Perform System Upgrade**.
The System Upgrade dialog appears and displays information about the upgrade and a list of users who are currently logged in to the system to be upgraded.
6. Verify the version of the target image (the upgrade image), and click **OK** to continue with the upgrade.
The System Upgrade dialog displays the upgrade status and the time remaining.
When a local DDR is upgrading, you must wait for the upgrade to complete before using DD System Manager to manage that system. If the system restarts, the upgrade

might continue after the restart, and DD System Manager displays the upgrade status after login. EMC recommends that you keep the System Upgrade progress dialog open until the upgrade completes or the system powers off. If you are upgrading DD OS Release 5.5 on a local system to a newer version, and if the system upgrade does not require a power off, a Login link appears when the upgrade is complete.

You can use DD System Manager to monitor an upgrade on a remote system. When the upgrade completes on a remote system, the System Upgrade dialog displays a **Close** button.

Note

DD OS Release 5.5 introduces a new on-disk index layout that enables support for new DDFS features. During the upgrade, the index grows to the new size required to support the existing index entries in the new format. This step can take up to 1 hour.

Note

To view the status of an upgrade using the CLI, enter the `system upgrade status` command. Log messages for the upgrade are stored in `/ddvar/log/debug/sm/em.info`.

7. If the system powers down, you must remove AC power from the system to clear the prior configuration. Unplug all of the power cables for 30 seconds and then plug them back in. The system powers on and reboots.
8. If the system does not automatically power on and there is a power button on the front panel, press the button.

Removing an upgrade package

A maximum of five upgrade packages can be uploaded to a system with DD System Manager. If the system you are upgrading contains five upgrade packages, you must remove at least one package before you can upgrade the system.

Procedure

1. Expand **DD Network** in the Navigation panel, and select the system you want to manage.
2. Select **Maintenance** > **System**.
3. From the list titled Upgrade Packages Available on this Data Domain System, select the package to remove. One package can be removed at a time.
4. Click **Remove Upgrade Package**.

Managing system licenses

Add system licenses using purchased license keys to enable Data Domain system features. Remove a system license when you are decommissioning a system.

Procedure

1. In the Navigation panel, expand **DD Network** and select a managed system.
2. Select **System Settings** > **Licenses**.

The Feature Licenses list displays the installed license keys and feature names.

3. To add a license, complete the following tasks.

- a. Click **Add Licenses**.
 - b. In the Add Licenses Key dialog box, type or paste one or more license keys in the License Key box. Type each key on its own line, or separate each key by a space or comma (DD System Manager automatically places each key on a new line).
 - c. Click **Add**.
The added licenses display in the Added license list.
Any errors are listed in the error license list. Select a license with an error to edit it. Select **Retry Failed License(s)** to retry the key. Otherwise, click **Done** to ignore the errors and return to the Feature Licenses list.
4. To delete a license, complete the following tasks.
 - a. In the Feature Licenses list, select one or more licenses to remove and click **Delete Selected Licenses**.
 - b. In the Warning dialog box verify the license(s) to delete and click **OK**.
The licenses are removed from the license list.

System storage management

System storage management features allow you to view the status and configuration of your storage space, flash a disk LED to facilitate disk identification, and change the storage configuration.

Viewing system storage information

The system automatically scans and inventories system storage so that you can view the status and inventory for all enclosures, disks, and RAID groups.

Procedure

1. Select a system in the Navigation panel.
2. Select **Hardware > Storage**.

The Storage view Status area shows the current status of the storage, such as Operational or Non-Operational, and any active alerts, which you can click to view alert details. Below the Status area are tabs that organize how the storage inventory is presented.

Overview tab

The Overview tab displays information for all disks in the selected Data Domain system organized by type. The categories that display are dependent on the type of storage configuration in use.

The Overview section lists the discovered storage in one or more of the following sections.

- **Active Tier**
Disks in the Active Tier are currently marked as usable by the Data Domain file system. Sections are organized by Disks in Use and Disks Not in Use.
- **Retention Tier**
If the optional EMC Data Domain Extended Retention (formerly DD Archiver) license is installed, this section shows the disks that are configured for Extended Retention

storage. Sections are organized by Disks in Use and Disks Not in Use. For more information, see the *EMC Data Domain Extended Retention Administration Guide*.

- **Usable Disks and Enclosures**
For systems with optional enclosures, this section shows the disks and enclosures that can be added to the system.
- **Failed/Foreign/Absent Disks (Excluding Systems Disks)**
Shows the disks that are in a failed state; these cannot be added to the system Active or Retention tiers.
- **Systems Disks**
Shows the disks where the DD OS resides when the Data Domain controller does not contain data storage disks.

Each section heading displays a summary of the storage configured for that section. The summary shows tallies for the total number of disks, disks in use, spare disks, reconstructing spare disks, available disks, and known disks.

Click a section plus (+) button to display detailed information, or click the minus (-) button to hide the detailed information.

Table 17 Disks In Use column label descriptions

Item	Description
Disk Group	The name of the disk group that was created by the file system (for example, dg1).
Status	The status of the disk (for example Normal, Warning).
Disks Reconstructing	The disks that are undergoing reconstruction, by disk ID (for example, 1.11).
Total Disks	The total number of usable disks (for example, 14).
Disks	The disk IDs of the usable disks (for example, 2.1-2.14).

Table 18 Disks Not In Use column label descriptions

Item	Description
Disk	The disk identifier. It can be: <ul style="list-style-type: none"> • The enclosure and disk number (in the form Enclosure Slot). • A gateway disk (devn). • A LUN.
Status	The status of the disk, for example In Use, Available, Spare.
Size	The data storage capacity of the disk when used in a Data Domain system. ^a
Manufacturer/Model	The manufacturer’s model designation. The display may include a model ID or 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 Number	The manufacturer’s serial number for the disk.

Table 18 Disks Not In Use column label descriptions (continued)

- a. The Data Domain convention for computing disk space defines one gibibyte as 230 bytes, giving a different disk capacity than the manufacturer's rating.

Status tab

The Status tab displays a summary status table showing the state of all system disks and another table that provides additional information on reconstructing disks.

Table 19 Disks Status table column label descriptions

Item	Description
Total	The total number of inventoried disks in the Data Domain system (including enclosures and gateway storage).
In Use	The number of disks currently in use by the file system.
Spare	The number of spare disks (available to replace failed disks).
Spare (reconstructing)	The number of disks that are in the process of data reconstruction (spare disks replacing failed disks).
Available	The number of disks that are available for allocation to an Active or Extended Retention storage tier.
Known	The number of known unallocated disks.
Unknown	The number of unknown unallocated disks.
Failed	The number of failed disks.
Foreign	The number of foreign disks.
Absent	The number of absent disks.

The following table describes the entries in the Reconstructing table.

Table 20 Reconstruction table column label descriptions

Item	Description
Disk	Identifies disks that are being reconstructed. Disk labels are of the format <i>enclosure.disk</i> . Enclosure 1 is the Data Domain system, and external shelves start numbering with enclosure 2. For example, the label 3.4 is the fourth disk in the second shelf.
Disk Group	Shows the RAID group (dg#) for the reconstructing disk.
Tier	The name of the tier where the failed disk is being reconstructed.
Time Remaining	The amount of time before the reconstruction is complete.
Percentage Complete	The percentage of reconstruction that is complete.

When a spare disk is available, the Data Domain file system automatically replaces a failed disk with a spare and begins the reconstruction process to integrate the spare into the RAID disk group. The disk use displays *Spare* and the status becomes *Reconstructing*. Reconstruction is performed on one disk at a time.

Disks tab

The Disks tab displays information on each of the system disks. You can filter the disks viewed to display all disks, disks in a specific tier, or disks in a specific group.

Table 21 Disks Status table column label descriptions

Item	Description
Disk	<p>The disk identifier, which can be:</p> <ul style="list-style-type: none"> • The enclosure and disk number (in the form <i>Enclosure.Slot</i>). • A gateway disk (dev <i>n</i>). • A LUN.
Status	<p>The status of the disk, which can be one of the following.</p> <ul style="list-style-type: none"> • Absent. No disk is installed in the indicated location. • Available. An available disk is allocated to the active or retention tier, but it is not currently in use. • Copy Recovery. The disk has a high error rate but is not failed. RAID is currently copying the contents onto a spare drive and will fail the drive once the copy reconstruction is complete. • Error. The disk has a high error rate but is not failed. The disk is in the queue for copy reconstruction. The state will change to Copy Recovery when copy reconstruction begins. • In-Use. The disk is being used for backup data storage. • Known. The disk is a supported disk that is ready for allocation. • Foreign. The disk has been assigned to a tier, but the disk data indicates the disk may be owned by another system. • Powered Off. The disk power has been removed by EMC Support. • Reconstruction. The disk is reconstructing in response to a <code>disk fail</code> command or by direction from RAID/SSM. • Spare. The disk is available for use as a spare. • Unknown. An unknown disk is not allocated to the active or retention tier. It might have been failed administratively or by the RAID system. • System. System disks store DD OS and system data. No backup data is stored on system disks.
Manufacturer/Model	<p>The manufacturer's model designation. The display may include a model ID or RAID type or other information depending on the vendor string sent by the storage array.</p>
Firmware	<p>The firmware level used by the third-party physical-disk storage controller.</p>
Serial Number	<p>The manufacturer's serial number for the disk.</p>

Physically locating a disk

If you have trouble determining which physical disk corresponds to a disk displayed in DD System Manager, you can use the beacon feature to flash an LED on the physical disk.

Procedure

1. Select the system in the Navigation panel.
2. Select **Hardware** > **Storage** > **Disks**.
3. Select a disk from the **Disks** table and click **Beacon**.

Note

You can select one disk at a time.

The Beaconsing Disk dialog box appears, and the LED light on the disk begins flashing.

4. Click **Stop** to stop the LED beaconing.

Configuring storage

Storage configuration features allow you add and remove storage expansion shelves from the active and retention tiers. Storage in an expansion shelf is not available for use until it is added to a tier.

Note

Additional storage requires the appropriate license or licenses and sufficient memory to support the new storage capacity. Error messages display if more licenses or memory is needed.

Procedure

1. Expand **DD Network** in the Navigation panel, and select a system.
2. Select **Hardware** > **Storage**.
3. In the Overview tab, click **Configure Storage**.
4. In the Configure Storage dialog box, select the storage to be added from the **Available Storage** list.
5. Select the appropriate Tier Configuration (Active or Retention) from the menu.

The maximum amount of storage that can be added to the active tier depends on the DD controller used.

Note

The two bars show the portion of licensed capacity (used and remaining) for each shelf model (ES20 and ES30).

6. Select the checkbox for the Shelf to be added.
7. Click the **Add to Tier** button.
8. Click **OK** to add the storage.

Note

To remove an added shelf, select it in the Tier Configuration list, click **Remove from Configuration**, and click **OK**.

Network connection management

Network connection management features allow you view and configure network interfaces, general network settings, and network routes.

Network interface management

Network interface management features allow you to manage the physical interfaces that connect the system to a network and create logical interfaces to support link aggregation, load balancing, and link failover.

Viewing interface information

The Interfaces tab allows you to manage physical and virtual interfaces, VLANs, DHCP, DDNS, and IP addresses and aliases.

Consider the following guidelines when managing IPv6 interfaces.

- The command-line interface (CLI) supports IPv6 for basic Data Domain network and replication commands, but not for backup and Extended Retention (*archive*) commands. CLI commands manage the IPv6 addresses. You can view IPv6 addresses using the DD System Manager, but you cannot manage IPv6 with the DD System Manager.
- 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.
- There are some restrictions for interfaces with IPv6 addresses. For example, the minimum MTU is 1280. If you try to set the MTU lower than 1280 on an interface with an IPv6 address, an error message appears and the interface is removed from service. An IPv6 address can affect an interface even though it is on a VLAN attached to the interface and not directly on the interface.

Procedure

1. In the Navigation panel, select the system to view or configure.
2. Select **Hardware > Network > Interfaces**.

The following table describes the information on the Interfaces tab.

Table 22 Interface tab label descriptions

Item	Description
Interface	The name of each interface associated with the selected system.
Enabled	Whether the interface is enabled. <ul style="list-style-type: none"> • Select Yes to enable the interface and connect it to the network.

Table 22 Interface tab label descriptions (continued)

Item	Description
	<ul style="list-style-type: none"> Select No to disable the interface and disconnect it from the network.
DHCP	Indicates if the interface is configured manually (no), by a DHCP (Dynamic Host Configuration Protocol) IPv4 server (v4), or by a DHCP IPv6 server (v6).
IP Address	IP address associated with the interface. The address used by the network to identify the interface. If the interface is configured through DHCP, an asterisk appears after this value.
Netmask	Netmask associated with the interface. Uses the standard IP network mask format. If the interface is configured through DHCP, an asterisk appears after this value.
Link	Whether the Ethernet connection is active (Yes/No).
Additional Info	Additional settings for the interface. For example, the bonding mode.
IPMI interfaces configured	Displays Yes or No and indicates if IPMI health monitoring and power management is configured for the interface.

- To filter the interface list by interface name, enter a value in the **Interface Name** field and click **Update**.

Filters support wildcards, such as eth*, veth*, or eth0*

- To filter the interface list by interface type, select a value from the **Interface Type** menu and click **Update**.
- To return the interfaces table to the default listing, click **Reset**.
- Select an interface in the table to populate the Interface Details area.

Table 23 Interface Details label descriptions

Item	Description
Auto-generated Addresses	Displays the automatically generated IPv6 addresses for the selected interface.
Autonegotiate	When this feature displays <i>Enabled</i> , the interface automatically negotiates Speed and Duplex settings. When this feature displays <i>Disabled</i> , then Speed and Duplex values must be set manually.
Cable	Shows whether the interface is Copper or Fiber.
	<p>Note</p> <p>Some interfaces must be up before the cable status is valid.</p>
Duplex	Used in conjunction with the Speed value to set the data transfer protocol. Options are Unknown, Full, Half.
Hardware Address	The MAC address of the selected interface. For example, 00:02:b3:b0:8a:d2.

Table 23 Interface Details label descriptions (continued)

Item	Description
Interface Name	Name of the selected interface.
MTU	MTU (Maximum Transfer Unit) value assigned to the interface.
Speed	Used in conjunction with the Duplex value to set the rate of data transfer. Options are Unknown, 10 Mb/s, 100 Mb/s, 1000 Mb/s, 10 Gb/s.
	<p>Note</p> <p>Auto-negotiated interfaces must be set up before speed, duplex, and supported speed are visible.</p>
Supported Speeds	Lists all of the speeds that the interface can use.

7. To view IPMI interface configuration and management options, click **View IPMI Interfaces**.

This link displays the **Maintenance > IPMI** configuration tab.

Physical interface names and limitations

The format of physical interface names varies on different Data Domain systems and option cards, and limitations apply to some interfaces.

- For most systems the physical interface name format is `ethxy`, where *x* is the slot number for an on-board port or an option card and *y* is an alphanumeric string. For example, `eth0a`.
- For most on-board NIC vertical interfaces, the top interface is named `eth0a` and the bottom interface is `eth0b`.
- For most on-board NIC horizontal interfaces, the left interface as viewed from the rear, is named `eth0a` and the right is named `eth0b`.
- DD990 systems provide four on-board interfaces: two on the top and two on the bottom. The top-left interface is `eth0a`, the top-right is `eth0b`, the bottom-left is `eth0c`, and the bottom-right is `eth0d`.
- DD2200 systems provide four on-board 1G Base-T NIC ports: `ethMa` (top left), `ethMb` (top right), `ethMc` (bottom left), and `ethMd` (bottom right).
- DD2500 systems provide six on-board interfaces. The four on-board 1G Base-T NIC ports are `ethMa` (top left), `ethMb` (top right), `ethMc` (bottom left), and `ethMd` (bottom right). The two on-board 10G Base-T NIC ports are `ethMe` (top) and `ethMf` (bottom).
- DD4200, DD4500, and DD7200 systems provide one on-board Ethernet port, which is `ethMa`.
- For systems ranging between DD140 and DD990, the physical interface names for I/O modules start at the top of the module or at the left side. The first interface is `ethxa`, the next is `ethxb`, the next is `ethxc`, and so forth.
- The port numbers on the horizontal DD2500 I/O modules are labeled in sequence from the end opposite the module handle (left side). The first port is labeled 0 and corresponds to physical interface name `ethxa`, the next is `1/ethxb`, the next is `2/ethxc`, and so forth.

- The port numbers on the vertical DD4200, DD4500, and DD7200 I/O modules are labeled in sequence from the end opposite the module handle (bottom). The first port is labeled 0 and corresponds to physical interface name ethxa, the next is 1/ethxb, the next is 2/ethxc, and so forth.

General interface configuration guidelines

Review the general interface configuration guidelines before configuring system interfaces.

- When supporting both backup and replication traffic, EMC recommends using different interfaces for each traffic type so that neither traffic type impacts the other.
- When replication traffic is expected to be less than 1 Gb/s, EMC recommends against using 10 GbE interfaces for replication traffic because 10 GbE interfaces are optimized for faster traffic.
- On DD4200, DD4500, and DD7200 systems that use IPMI, EMC recommends that interface ethMa be reserved for IPMI traffic and system management traffic (using protocols such as HTTP, Telnet, and SSH). Backup data traffic should be directed to other interfaces.

Configuring physical interfaces

You must configure at least one physical interface before the system can connect to a network.

Procedure

1. In the Navigation panel, select the system to configure.
2. Select **Hardware** > **Network** > **Interfaces**.
3. Select an interface to configure.

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.

4. Click **Configure**.
5. In the Configure Interface dialog, determine how the interface IP address is to be set:
 - Use DHCP to assign the IP address—in the IP Settings area, select **Obtain IP Address using DHCP** and select either **DHCPv4** for IPv4 access or **DHCPv6** for IPv6 access.
Setting a physical interface to use DHCP automatically enables the interface.

Note

If you choose to obtain the network settings through DHCP, you can manually configure the hostname at **Hardware** > **Network** > **Settings** or with the `net set hostname` command. You must manually configure the host name when using DHCP over IPv6.

- Specify IP Settings manually—in the IP Settings area, select **Manually configure IP Address**.
The **IP Address** and **Netmask** fields become active.
 - a. Enter an IPv4 or IPv6 address.

The Internet Protocol (IP) address is the numerical label assigned to the interface. For example, 192.168.10.23.

Note

You can assign just one IP address to an interface with this procedure. If you assign another IP address, the new address replaces the old address. To attach an additional IP address to an interface, create an IP alias.

- b. If you entered an IPv4 address, enter a netmask address.

The netmask specifies the subnet portion of an IPv4 address that is assigned to the interface. If the interface is configured through DHCP, an asterisk appears after this value.

The format is typically 255.255.255.0. If you do not specify a netmask, the selected system uses the netmask format determined by the TCP/IP address class (A,B,C) you are using.

6. Specify Speed/Duplex settings.

The combination of speed and duplex settings define the rate of data transfer through the interface. Select one of these options:

- **Autonegotiate Speed/Duplex** — Select this option to allow the network interface card to autonegotiate the line speed and duplex setting for an interface. Autonegotiation is *not* supported on the following DD2500, DD4200, DD4500, and DD7200 I/O modules:
 - Dual Port 10GbE SR Optical with LC connectors (using SFPs)
 - Dual Port 10GbE Direct Attach Copper (SFP+ cables)
 - Quad port 2 port 1GbE Copper (RJ45) / 2 port 1GbE SR Optical
- **Manually configure Speed/Duplex** — Select this option to manually set an interface data transfer rate. Select the speed and duplex from the menus.
 - Duplex options are half-duplex, full-duplex, and unknown.
 - Speed options listed are limited to the capabilities of the hardware device. Options are 10 Mb, 100 Mb, 1000 Mb (1 Gb), 10 Gb, and unknown. The 10G Base-T hardware supports only the 100 Mb, 1000 Mb and 10 Gb settings.
 - Half-duplex is only available for 10 Mb and 100 Mb speeds.
 - 1000 Mb and 10 Gb line speeds require full-duplex.
 - On DD2500, DD4200, DD4500, and DD7200 10GbE I/O modules, copper interfaces support only the 10 Gb speed setting.
 - The default setting for 10G Base-T interfaces is Autonegotiate Speed/Duplex. If you manually set the speed to 1000 Mb or 10 Gb, you must set the Duplex setting to Full.

7. Specify the MTU (Maximum Transfer Unit) size for the physical (Ethernet) interface.

Do the following:

- Click the **Default** button to return the setting to the default value.
- Ensure that all of your network components support the size set with this option.

8. Optionally, select **Dynamic DNS Registration**.

Dynamic DNS (DDNS) is a protocol that registers local IP addresses on a Domain Name System (DNS) server. In this release, DD System Manager supports Windows mode DDNS. To use UNIX mode DDNS, use the `net ddns` CLI command.

The DDNS must be registered to enable this option.

Note

This option disables DHCP for this interface.

9. Click **Next**.

The Configure Interface Settings summary page appears. The values listed reflect the new system and interface state, which are applied after you click Finish.

10. Click **Finish** and **OK**.

MTU size values

The MTU size must be set properly to optimize the performance of a network connection. An incorrect MTU size can negatively affect interface performance.

Supported values for setting the maximum Transfer Unit (MTU) size for the physical (Ethernet) interface range from 350 to 9000. For 100 Base-T and gigabit networks, 1500 is the standard default.

Note

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

Note

The minimum MTU for IPv6 interfaces is 1280. The interface fails if you try to set the MTU lower than 1280.

Moving a static IP address

A specific static IP address must be assigned to only one interface on a system. A static IP address must be properly removed from an interface before it is configured on another interface.

Procedure

1. In the Navigation panel, select the system to configure.
2. If the interface that hosts the static IP address is part of a DD Boost interface group, remove the interface from that group.
3. Select **Hardware** > **Network** > **Interfaces**.
4. Remove the static IP address that you want to move.
 - a. Select the interface that is currently using the IP address you want to move.
 - b. In the Enabled column, select **No** to disable the interface.
 - c. Click **Configure**.
 - d. Set the IP Address to 0.

Note

Set the IP address to 0 when there is no other IP address to assign to the interface. The same IP address must not be assigned to multiple interfaces.

- e. Click **Next**, and click **Finish**.
5. Add the removed static IP address to another interface.
 - a. Select the interface to which you want to move the IP address.
 - b. In the Enabled column, select **No** to disable the interface.
 - c. Click **Configure**.
 - d. Set the IP Address to the match the static IP address you removed.
 - e. Click **Next**, and click **Finish**.
 - f. In the Enabled column, select **Yes** to enable the updated interface.

Virtual interface configuration guidelines

Virtual interface configuration guidelines apply to failover and aggregate virtual interfaces. There are additional guidelines that apply to either failover or aggregate interfaces but not both.

- The *virtual-name* must be in the form `vethx` where *x* is a number. The recommended maximum number is 99 because of name size limitations.
- You can create as many virtual interfaces as there are physical interfaces.
- Each interface used in a virtual interface must first be disabled. An interface that is part of a virtual interface is seen as disabled for other network configuration options.
- After a virtual interface is destroyed, the physical interfaces associated with it remain disabled. You must manually re-enable the physical interfaces.
- The number and type of cards installed determines the number of Ethernet ports available.
- Each physical interface can belong to one virtual interface.
- A system can support multiple mixed failover and aggregation virtual interfaces, subject to the restrictions above.
- Virtual interfaces must be created from identical physical interfaces. For example, all copper, all optical, all 1 Gb, or all 10 Gb. However, 1 Gb interfaces support bonding a mix of copper and optical interfaces. This applies to virtual interfaces across different cards with identical physical interfaces, except for Chelsio cards. For Chelsio cards, only failover is supported, and that is only across interfaces on the same card.
- Failover and aggregate links improve network performance and resiliency by using two or more network interfaces in parallel, thus increasing the link speed and reliability over that of a single interface.
- Remove functionality is available using the **Configure** button. Click a virtual interface in the list of interfaces on the Interfaces tab and click **Configure**. From the list of interfaces in the dialog box, clear the checkbox for the interface to remove it from bonding (failover or aggregate), and click **Next**.
- On DD4200, DD4500, and DD7200 systems, the ethMa interface does not support failover or link aggregation.

Guidelines for configuring a virtual interface for link aggregation

Link aggregation provides improved network performance and resiliency by using one or more network interfaces in parallel, thus increasing the link speed and reliability over

that of a single interface. These guidelines are provided to help you optimize your use of link aggregation.

- Changes to disabled Ethernet interfaces flush the routing table. It is recommended that you make interface changes only during scheduled maintenance downtime. Afterwards, reconfigure the routing rules and gateways.
- Enable aggregation on an existing virtual interface by specifying the physical interfaces and mode and giving it an IP address.
- 10 Gb single-port optical Ethernet cards do not support link aggregation.
- 1 GbE and 10 GbE interfaces cannot be aggregated together.
- Copper and optical interfaces cannot be aggregated together.
- DD2500 on-board 10G Base-T interfaces ethMe and ethMf do not support link aggregation.
- On DD4200, DD4500, and DD7200 systems, the ethMA interface does not support link aggregation.

Guidelines for configuring a virtual interface for failover

Link failover provides improved network stability and performance by identifying backup interfaces that can support network traffic when the primary interface is not operating. These guidelines are provided to help you optimize your use of link failover.

- A primary interface must be part of the failover. If a primary interface removal is attempted from a failover, an error message appears.
- When a primary interface is used in a failover configuration, it must be explicitly specified and must also be a bonded interface to the virtual interface. If the primary interface goes down and multiple interfaces are still available, the next interface is randomly selected.
- All interfaces in a virtual interface must be on the same physical network. Network switches used by a virtual interface must be on the same physical network.
- The recommended number of physical interfaces for failover is greater than one. You can, however, configure one primary interface and one or more failover interfaces, except with the following:
 - 10 Gb CX4 Ethernet card, which are restricted to one primary interface and one failover interface from the same card, and
 - 10 Gb single-port optical Ethernet cards, which cannot be used.
- On DD4200, DD4500, and DD7200 systems, the ethMA interface does not support link failover.

Virtual interface creation

Create a virtual interface to support link aggregation or failover. The virtual interface serves as a container for the links to be aggregated or associated for failover.

Creating a virtual interface for link aggregation

Create a virtual interface for link aggregation to serve as a container to associate the links that participate in aggregation.

A link aggregation interface must specify a link bonding mode and may require a hash selection. For example, you might enable link aggregation on virtual interface *veth1* to physical interfaces *eth1* and *eth2* in mode LACP (Link Aggregation Control Protocol) and hash XOR-L2L3.

Procedure

1. In the Navigation panel, select the system to configure.
2. Select **Hardware** > **Network** > **Interfaces**.
3. In the Interfaces table, disable the physical interface where the virtual interface is to be added by clicking **No** in the **Enabled** column.
4. From the **Create** menu, select **Virtual Interface**.
5. In the Create Virtual Interface dialog box, specify a virtual interface name in the **veth** box.

Enter a virtual interface name in the form *vethx*, where *x* is a unique ID (typically one or two digits). A typical full virtual interface name with VLAN and IP Alias is *veth56.3999:199*. The maximum length of the full name is 15 characters. Special characters are not allowed. Numbers must be between 0 and 4094, inclusively.

6. Select **Aggregate** from the **Bonding Type** menu.
-

Note

Registry settings can be different from the bonding configuration. When interfaces are added to the virtual interface, the information is not sent to the bonding module until the virtual interface is given an IP address and brought up. Until that time the registry and the bonding driver configuration are different.

7. From the **General** tab, specify the **Bonding Mode**.

Specify the mode that is compatible with the requirements of the system to which the interfaces are directly attached.

- **Round-robin**
Transmit packets in sequential order from the first available link through the last 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 Ether channel (trunk) and given a hash via the Load Balance parameter.
- **LACP**
Link Aggregation Control Protocol is similar to Balanced, except that it uses a control protocol that communicates to the other end and coordinates which links within the bond are available for use. LACP provides a kind of heartbeat failover and must be configured at both ends of the link.

8. If you selected Balanced or LACP mode, specify a bonding hash type.

From the **General** tab, select from the **Bonding Hash** menu.

Options are: XOR-L2, XOR-L2L3, or XOR-L3L4.

XOR-L2 transmits through a bonded interface with an XOR hash of Layer 2 (inbound and outbound MAC addresses).

XOR-L2L3 transmits through a bonded interface with an XOR hash of Layer 2 (inbound and outbound MAC addresses) and Layer 3 (inbound and outbound IP addresses).

XOR-L3L4 transmits through a bonded interface with an XOR hash of Layer 3 (inbound and outbound IP addresses) and Layer 4 (inbound and outbound ports).

9. To select an interface to add to the aggregate configuration, select the checkbox that corresponds to the interface, and then click **Next**.

The Create virtual interface *veth_name* dialog appears.

10. Enter an IP address, or enter 0 to specify no IP address.

The Internet Protocol (IP) address is the numerical label assigned to the interface. For example, 192.168.10.23.

11. Enter a netmask address.

The netmask is the subnet portion of the IP address that is assigned to the interface.

The format is typically 255.255.255.0. If you do not specify a netmask, the system uses the default netmask determined by the TCP/IP address class (A, B, C) you are using.

12. Specify Speed/Duplex options.

The combination of speed and duplex settings define the rate of data transfer through the interface. Select either:

- **Autonegotiate Speed/Duplex**
Select this option to allow the network interface card to autonegotiate the line speed and duplex setting for an interface.
- **Manually configure Speed/Duplex**
Select this option to manually set an interface data transfer rate.
 - Duplex options are half-duplex or full-duplex.
 - Speed options listed are limited to the capabilities of the hardware device. Options are 10 Base-T, 100 Base-T, 1000 Base-T (Gigabit), and 10,000 (10 Gb).
 - Half-duplex is only available for 10 Base-T and 100 Base-T speeds.
 - 1000 and 10000 line speeds require full-duplex.
 - Optical interfaces require the Autonegotiate option.
 - The 10 GbE copper NIC default is 10 Gb. If a copper interface is set to 1000 or 10000 line speed, duplex must be full-duplex.

13. Specify MTU Settings.

Do the following:

- Click the **Default** button to return the setting to the default value.
- Ensure that all of your network components support the size set with this option.

14. Optionally, select Dynamic DNS Registration option.

Dynamic DNS (DDNS) is a protocol that registers local IP addresses on a Domain Name System (DNS) server. In this release, DD System Manager supports Windows mode DDNS. To use UNIX mode DDNS, use the `net ddns` CLI command.

The DDNS must be registered to enable this option.

15. Click **Next**.

The Configure Interface Settings summary page appears. The values listed reflect the new system and interface state.

16. Click **Finish** and **OK**.

Creating a virtual interface for link failover

Create a virtual interface for link failover to serve as a container to associate the links that will participate in failover.

The failover-enabled virtual interface represents a group of secondary interfaces, one of which can be specified as the primary. The system makes the primary interface the active interface whenever the primary interface is operational. A configurable Down Delay failover option allows you to configure a failover delay in 900 millisecond intervals. The failover delay guards against multiple failovers when a network is unstable.

Procedure

1. In the Navigation panel, select the system to configure.
2. Select **Hardware** > **Network** > **Interfaces**.
3. In the **Interfaces** table, disable the physical interface to which the virtual interface is to be added by clicking **No** in the **Enabled** column.
4. From the **Create** menu, select **Virtual Interface**.
5. In the Create Virtual Interface dialog box, specify a virtual interface name in the **veth** box.
 Enter a virtual interface name in the form `vethx`, where *x* is a unique ID (typically one or two digits). A typical full virtual interface name with VLAN and IP Alias is `veth56.3999:199`. The maximum length of the full name is 15 characters. Special characters are not allowed. Numbers must be between 0 and 4094, inclusively.
6. Select **Failover** from the **Bonding Type** menu.
7. In the Select an interface to add to the failover configuration, select the corresponding to the interface and click **Next**. Virtual aggregate interfaces can be used for failover.
 The Create virtual interface `veth_name` dialog appears.
8. Enter an IP address, or enter 0 to specify no IP address.
 The Internet Protocol (IP) address is the numerical label assigned to the interface. For example, 192.168.10.23.
9. Enter a netmask address.
 The netmask is the subnet portion of the IP address that is assigned to the interface. The format is typically 255.255.255.0. If you do not specify a netmask, the selected system uses the default netmask defined by the TCP/IP address class (A,B,C) you are using.
10. Specify the Speed/Duplex options.
 The combination of speed and duplex settings defines the rate of data transfer through the interface. Select either:
 - **Autonegotiate Speed/Duplex** to allow the network interface card to autonegotiate the line speed and duplex setting for an interface.
 - **Manually configure Speed/Duplex** to manually set an interface data-transfer rate.
 - Duplex options are either half duplex or full duplex.
 - Speed options listed are limited to the capabilities of the hardware device. Options are 10 Base-T, 100 Base-T, 1000 Base-T (Gigabit), and 10,000 (10 Gb).

- Half-duplex is available for 10 Base-T and 100 Base-T speeds only.
- 1000 and 10000 line speeds require full-duplex.
- Optical interfaces require the Autonegotiate option.
- The copper interface default is 10 Gb. If a copper interface is set to 1000 or 10000 line speed, the duplex must be full-duplex.

11. Specify MTU settings.

Do the following:

- Click the **Default** button to return the setting to the default value.
- Ensure that all of your network path components support the size set with this option.

12. Optionally, select Dynamic DNS Registration option.

Dynamic DNS (DDNS) is a protocol that registers local IP addresses on a Domain Name System (DNS) server. In this release, DD System Manager supports Windows mode DDNS. To use UNIX mode DDNS, use the `net ddns` CLI command.

The DDNS must be registered to enable this option.

Note

This option disables DHCP for this interface.

13. Click **Next**.

The Configure Interface Settings summary page appears. The values listed reflect the new system and interface state.

14. Complete the Interface, click **Finish** and **OK**.

Modifying a virtual interface

After you create a virtual interface, you can update the settings to respond to network changes or resolve issues.

Procedure

1. In the Navigation panel, select the system to configure.
2. Select **Hardware** > **Network** > **Interfaces**.
3. In the Interfaces column, select the interface and disable the virtual interface by clicking **No** in the **Enabled** column. Click **OK** in the warning dialog.
4. In the **Interfaces** column, select the interface and click **Configure**.
5. In the **Configure Virtual Interface** dialog, change the settings.
6. Click **Next** and **Finish**.

Configuring a VLAN

Create a new VLAN interface from either a physical interface or a virtual interface.

The recommended total VLAN count is 80. You can create up to 100 interfaces (minus the number of aliases, physical and virtual interfaces) before the system prevents you from creating any more.

Procedure

1. In the Navigation panel, select the system to configure.
2. Select **Hardware > Network > Interfaces**.
3. In the interfaces table, select the interface to which you want to add the VLAN.
The interface you select must be configured with an IP address before you can add a VLAN.
4. Click **Create** and select the **VLAN** option.
5. In the Create VLAN dialog box, specify a VLAN ID by entering a number in the **ID** field.
The range of a VLAN ID is between 1 and 4094 inclusive.
6. Enter an IP address, or enter 0 to specify no IP address.
The Internet Protocol (IP) address is the numerical label assigned to the interface. For example, 192.168.10.23.
7. Enter a netmask address.
The netmask is the subnet portion of the IP address that is assigned to the interface. The format is typically 255.255.255.0. If you do not specify a netmask, the selected system uses the default netmask determined by the TCP/IP address class (A, B, or C) you are using.
8. Specify MTU Settings.
The VLAN MTU must be less than or equal to the MTU defined for the physical or virtual interface to which it is assigned. If the MTU defined for the supporting physical or virtual interface is reduced below the configured VLAN value, the VLAN value is automatically reduced to match the supporting interface. If the MTU value for the supporting interface is increased above the configured VLAN value, the VLAN value is unchanged.
Do the following:
 - Click **Default** to return the setting to the default value.
 - Specify a specific MTU size. DD System Manager does not accept an MTU size that is larger than that defined for the physical or virtual interface to which the VLAN is assigned.
9. Specify Dynamic DNS Registration option.
Dynamic DNS (DDNS) is a protocol that registers local IP addresses on a Domain Name System (DNS) server. In this release, DD System Manager supports Windows mode DDNS. To use UNIX mode DDNS, use the `net ddns` CLI command.
The DDNS must be registered to enable this option.
10. Click **Next**.
The **Configure Interface Settings** summary page appears. The values listed reflect the new system and interface state.
11. Click **Finish** and **OK**.

Modifying a VLAN interface

After you create a VLAN interface, you can update the settings to respond to network changes or resolve issues.

Procedure

1. In the Navigation panel, select the system to configure.
2. Select **Hardware > Network > Interfaces**.
3. In the **Interfaces** column, select the checkbox of the interface and disable the VLAN interface by clicking **No** in the **Enabled** column. Click **OK** in the warning dialog box.
4. In the Interfaces column, select the checkbox of the interface and click **Configure**.
5. In the **Configure VLAN Interface** dialog box, change the settings.
6. Click **Next** and **Finish**.

Configuring an IP alias

An IP alias assigns an additional IP address to a physical interface, a virtual interface, or a VLAN.

The recommended total number of IP aliases, VLAN, physical, and virtual interfaces that can exist on the system is 80. Although up to 100 interfaces are supported, as the maximum number is approached, you might notice slowness in the display.

Procedure

1. In the Navigation panel, select the system to configure.
2. Select **Hardware > Network > Interfaces**.
3. Click the **Create** menu and select the IP Alias option.
The Create IP Alias dialog box appears.
4. Specify an IP alias ID by entering a number in the **eth0a** field.
Requirements are 1 to 4094 inclusive.
5. Enter an IPv4 or IPv6 address.
6. If you entered an IPv4 address, enter a netmask address.

The netmask specifies the subnet portion of the IP address that is assigned to the interface.

The format is typically 255.255.255.0. If you do not specify a netmask, the selected system uses the default netmask determined by the TCP/IP address class (A, B, or C) you are using.

7. Specify Dynamic DNS Registration option.

Dynamic DNS (DDNS) is a protocol that registers local IP addresses on a Domain Name System (DNS) server. In this release, DD System Manager supports Windows mode DDNS. To use UNIX mode DDNS, use the `net ddns` CLI command.

The DDNS must be registered to enable this option.

8. Click **Next**.

The Configure Interface Settings summary page appears. The values listed reflect the new system and interface state.

9. Click **Finish** and **OK**.

Modifying an IP alias interface

After you create an IP alias, you can update the settings to respond to network changes or resolve issues.

Procedure

1. In the Navigation panel, select the system to configure.
2. Select **Hardware** > **Network** > **Interfaces**.
3. In the **Interfaces** column, select the checkbox of the interface and disable the IP alias interface by clicking **No** in the **Enabled** column. Click **OK** in the warning dialog box.
4. In the **Interfaces** column, select the checkbox of the interface and click **Configure**.
5. In the Configure IP Alias dialog box, change the settings as described in the procedure for creating an IP Alias.
6. Click **Next** and **Finish**.

Registering interfaces with DDNS

Dynamic DNS (DDNS) is a protocol that registers local IP addresses on a Domain Name System (DNS) server.

In this release, DD System Manager supports Windows mode DDNS. To use UNIX mode DDNS, use the `net ddns` CLI command. You can do the following.

- Manually register (add) configured interfaces to the DDNS registration list.
- Remove interfaces from the DDNS registration list.
- Enable or disable DNS updates.
- Display whether DDNS registration is enabled or not.
- Display interfaces in the DDNS registration list.

Procedure

1. In the Navigation panel, select the system to configure.
2. Select **Hardware** > **Network** > **Interfaces**.
3. Click **DDNS Registration**.
4. In the DDNS Registration dialog box, to add an interface to the DDNS, click **Add**.
The Add Interface dialog box appears.
 - a. Enter a name in the **Interface** field.
 - b. Click **OK**.
5. Optionally, to remove an interface from the DDNS:
 - a. Select the interface to remove, and click **Remove**.
 - b. In the Confirm Remove dialog box, click **OK**.
6. Specify the DDNS Status.
 - Select **Enable** to enable updates for all interfaces already registered.
 - Click **Default** to select the default settings for DDNS updates.
 - Clear **Enable** to disable DDNS updates for the registered interfaces.

7. To complete the DDNS registration, click **OK**.

Destroying an interface

You can use DD System Manager to destroy or delete virtual, VLAN, and IP alias interfaces.

When a virtual interface is destroyed, the system deletes the virtual interface, releases its bonded physical interface, and deletes any VLANs or aliases attached to the virtual interface. When you delete a VLAN interface, the OS deletes the VLAN and any IP alias interfaces that are created under it. When you destroy an IP alias, the OS deletes only that alias interface.

Procedure

1. In the Navigation panel, select the system to configure.
2. Select **Hardware > Network > Interfaces**.
3. Click the box next to the interface to destroy (Virtual or VLAN or IP Alias).
4. Click **OK** to confirm.

Viewing an interface hierarchy in the tree view

The Tree View dialog displays the association between physical and virtual interfaces.

Procedure

1. In the Navigation panel, select the system to view.
2. Select **Hardware > Network > Interfaces**.
3. Click **Tree View**.
4. In the Tree View dialog box, select the plus or minus boxes to expand or contract the tree view that shows the hierarchy.
5. Click **Close** to exit this view.

General network settings management

The configuration settings for hostname, domain name, search domains, host mapping, and DNS list are managed together on the Settings tab.

Viewing network settings information

The Settings tab displays the current configuration for the hostname, domain name, search domains, host mapping, and DNS.

Procedure

1. In the Navigation panel, select the system to view or configure.
2. Select **Hardware > Network > Settings**.

The Settings view displays Host Settings, Search Domain, and Host Mapping options.

Results

The Settings tab displays the following information.

Host Settings

Host Name

The hostname of the selected system.

Domain Name

The fully qualified domain name associated with the selected system.

Search Domain List

Search Domain

A list of search domains that the selected system uses. The system applies the search domain as a suffix to the hostname.

Hosts Mapping

IP Address

IP address of the host to resolve.

Host Name

Hostnames associated with the IP address.

DNS List

DNS IP Address

Current DNS IP addresses associated with the selected system. An asterisk (*) indicates that the IP addresses were assigned through DHCP.

Setting the DD System Manager hostname

You can configure the DD System Manager hostname and domain name manually, or you can configure DD OS to automatically receive the host and domain names from a Dynamic Host Configuration Protocol (DHCP) server.

One advantage to manually configuring the host and domain names is that you remove the dependency on the DHCP server and the interface leading to the DHCP server. To minimize the risk of service interruption, EMC recommends that you manually configure the host and domain names.

When configuring the hostname and domain name, consider the following guidelines.

- Do not include an underscore in the hostname; it is incompatible with some browsers.
- Replication and CIFS authentication must be reconfigured after you change the names.
- If a system was previously added without a fully qualified name (no domain name), a domain name change requires that you remove and add the affected system or update the Search Domain List to include the new domain name.

Procedure

1. In the Navigation panel, select the system to configure.
2. Select **Hardware** > **Network** > **Settings**.
3. Click **Edit** in the **Host Settings** area. The Configure Host dialog box appears.
4. To manually configure the host and domain names:
 - a. Select **Manually configure the host**.
The DNS IP address checkboxes become active.
 - b. Enter a hostname in the **Host Name** box.

For example, `id##.yourcompany.com`

- c. Enter a domain name in the **Domain Name** box.

This is the domain name associated with your Data Domain system and, usually, your company's domain name. For example, *yourcompany.com*

- d. Click **OK**.

The system displays progress messages as the changes are applied.

5. To obtain the host and domain names from a DHCP server, select **Obtain Settings using DHCP** and click **OK**.

At least one interface must be configured to use DHCP.

Managing the domain search list

Use the domain search list to define which domains the system can search.

Procedure

1. In the Settings view, click **Edit** in the Search Domain List area.
2. To add a search domain using the Configure Search Domains dialog box:
 - a. Click Add (+).
 - b. In the Add Search Domain dialog box, enter a name in the **Search Domain** box.
For example, `id##.yourcompany.com`
 - c. Click **OK**.
The system adds the new domain to the list of searchable domains.
 - d. Click **OK** to apply changes and return to the Settings view.
3. To remove a search domain using the Configure Search Domains dialog box:
 - a. Select the search domain to remove.
 - b. Click Delete (X).
The system removes the selected domain from the list of searchable domains.
 - c. Click **OK** to apply changes and return to the Settings view.

Adding and deleting host maps

A host map links an IP address to a hostname, so that either the IP address or the hostname can be used to specify the host.

Procedure

1. Select **Hardware > Network > Settings**.
2. To add a host map, do the following.
 - a. In the Hosts Mapping area, click **Add**.
 - b. In the Add Hosts dialog, enter the IP address of the host in the **IP Address** box.
The Internet Protocol (IP) Address is the numerical label assigned to the interface, such as 192.168.10.23.
 - c. Click Add (+).
 - d. In the Add Host dialog, enter a hostname in the **Host Name** box for the listed system, such as `id##.yourcompany.com`.

- e. Click **OK** to add the new hostname to the Host Name list.
- f. Click **OK** to return to the Settings tab.
3. To delete a host map, do the following.
 - a. In the Hosts Mapping area, select the host mapping to delete.
 - b. Click **Delete**.
 - c. In the Delete Hosts dialog, click **Delete** to confirm.
Confirmation messages appear.
 - d. Click **Close** after the Completed message appears.

Configuring DNS IP addresses

DNS IP addresses specify the DNS servers the system can use to get IP addresses for host names that are not in the host mapping table.

You can configure the DNS IP addresses manually, or you can configure DD OS to automatically receive IP addresses from a DHCP server. One advantage to manually configuring DNS IP addresses is that you remove the dependency on the DHCP server and the interface leading to the DHCP server. To minimize the risk of service interruption, EMC recommends that you manually configure the DNS IP addresses.

Procedure

1. In the Navigation panel, select the system to configure.
2. Select **Hardware > Network > Settings**.
3. Click **Edit** in the **DNS List** area.
4. To manually add a DNS IP address:
 - a. Select **Manually configure DNS list**.
The DNS IP address checkboxes become active.
 - b. Click Add (+).
 - c. In the Add DNS dialog box, enter the DNS IP address to add.
 - d. Click **OK**.
The system adds the new IP address to the list of DNS IP addresses.
 - e. Click **OK** to apply the changes.
5. To delete a DNS IP address from the list:
 - a. Select **Manually configure DNS list**.
The DNS IP address checkboxes become active.
 - b. Select the DNS IP address to delete and click Delete (X).
The system removes the IP address from the list of DNS IP addresses.
 - c. Click **OK** to apply the changes.
6. To obtain DNS addresses from a DHCP server, select **Obtain DNS using DHCP** and click **OK**.
At least one interface must be configured to use DHCP.

Network route management

Routes determine the path taken to transfer data to and from the localhost (the Data Domain system) to another network or host.

Data Domain systems do not generate or respond to any of the network routing management protocols (RIP, EGRP/EIGRP, and BGP). The only routing implemented on a Data Domain system is based upon the internal route table, in which the administrator may define a specific network or subnet that a physical interface (or interface group) uses.

Data Domain systems use source-based routing, which means that outbound network packets that match the subnet of multiple interfaces are routed only over the physical interface from which they originated.

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

Note

Routing for connections initiated from the Data Domain system, such as for replication, depends on the source address used for interfaces on the same subnet. To force traffic for a specific interface to a specific destination (even if that interface is on the same subnet as other interfaces), configure a static routing entry between the two systems: this static routing overrides source routing.

Viewing route information

The Routes tab displays the default gateways, static routes, and dynamic routes.

Procedure

1. In the Navigation panel, select the system to view or configure.
2. Select **Hardware > Network > Routes**.

Results

The Static Routes area lists the route specification used to configure each static route. The Dynamic Routes table lists information for each of the dynamically assigned routes.

Table 24 Dynamic Routes column label descriptions

Item	Description
Destination	The destination host/network where the network traffic (data) is sent.
Gateway	The address of the router in the DD network, or 0.0.0.0 if no gateway is set.
Genmask	The netmask for the destination net. Set to 255.255.255.255 for a host destination and 0.0.0.0 for the default route.
Flags	Possible flags include: U—Route is up, H—Target is a host, G —Use gateway, R —Reinstate route for dynamic routing, D—Dynamically installed by daemon or redirect, M —Modified from routing daemon or redirect, A —Installed by addrconf, C —Cache entry, and ! —Reject route.

Table 24 Dynamic Routes column label descriptions (continued)

Item	Description
Metric	The distance to the target (usually counted in hops). Not used by the DD OS, but might be needed by routing daemons.
MTU	Maximum Transfer Unit (MTU) size for the physical (Ethernet) interface.
Window	Default window size for TCP connections over this route.
IRTT	Initial RTT (Round Trip Time) used by the kernel to estimate the best TCP protocol parameters without waiting on possibly slow answers.
Interface	Interface name associated with the routing interface.

Setting the default gateway

You can configure the default gateway manually, or you can configure DD OS to automatically receive the default gateway IP addresses from a DHCP server.

One advantage to manually configuring the default gateway is that you remove the dependency on the DHCP server and the interface leading to the DHCP server. To minimize the risk of service interruption, EMC recommends that you manually configure the default gateway IP address.

Procedure

1. In the Navigation panel, select the system to configure.
2. Select **Hardware** > **Network** > **Routes**.
3. Click **Edit** next to the default gateway type (IPv4 or IPv6) you want to configure.
4. To manually configure the default gateway address:
 - a. Select **Manually Configure**.
 - b. Enter the gateway address in the **Gateway** boxes.
 - c. Click **OK**.
5. To obtain the default gateway address from a DHCP server, select **Use DHCP value** and click **OK**.

At least one interface must be configured to use DHCP.

Creating static routes

Static routes define destination hosts or networks that they system can communicate with.

Procedure

1. In the Navigation panel, select the system to configure.
2. Select **Hardware** > **Network** > **Routes**.
3. Click **Create** in the Static Routes area.
4. In the **Create Routes** dialog box, select the interface you want to host the static route and click **Next**.
5. Specify the Destination. Select one of the following:
 - To specify a destination network, select **Network** and enter the network address and netmask for the destination network.

- To specify a destination host, select **Host** and enter the hostname or IP address of the destination host.
6. Optionally, specify the gateway to use to connect to the destination network or host.
 - a. Select **Specify different gateway for this route**.
 - b. Enter the gateway address.
 7. Review the configuration and click **Next**.
The Create Routes Summary page appears. The values listed reflect the new configuration.
 8. Click **Finish**.
 9. After the process is completed, click **OK**.
The new route specification is listed in the Route Spec list.

Deleting static routes

Delete a static route when you no longer want the system to communicate with a destination host or network.

Procedure

1. In the Navigation panel, select the system to configure.
2. Select **Hardware > Network > Routes**.
3. Select the Route Spec of the route specification to delete.
4. Click **Delete**.
5. Click **Delete** to confirm and then click **Close**.

The selected route specification is removed from the Route Spec list.

System passphrase management

The system passphrase is a key that allows a Data Domain system to be transported with encryption keys on the system. The encryption keys protect the data and the system passphrase protects the encryption keys.

The system passphrase is a human-readable (understandable) key (like a smart card) which is used to generate a machine usable AES 256 encryption key. If the system is stolen in transit, an attacker cannot easily recover the data; at most, they can recover the encrypted user data and the encrypted keys.

The passphrase is stored internally on a hidden part the Data Domain storage subsystem. This allows the Data Domain system to boot and continue servicing data access without any administrator intervention.

Setting the system passphrase

The system passphrase must be set before the system can support data encryption or request digital certificates.

Before you begin

No minimum system passphrase length is configured when DD OS is installed, but the CLI provides a command to set a minimum length. To determine if a minimum length is configured for the passphrase, enter the `system passphrase option show` CLI command.

Procedure

1. Select a system, and select **System Settings** > **Access Management** > **Administrator Access**.

If the system passphrase is not set, the **Set Passphrase** button appears in the Passphrase area. If a system passphrase is configured, the **Change Passphrase** button appears, and your only option is to change the passphrase.

2. Click the **Set Passphrase** button.

The Set Passphrase dialog appears.

3. Enter the system passphrase in the boxes and click **Next**.

If a minimum length is configured for the system passphrase, the passphrase you enter must contain the minimum number of characters.

Results

The system passphrase is set and the **Change Passphrase** button replaces the **Set Passphrase** button.

Changing the system passphrase

The administrator can change the passphrase without having to manipulate the actual encryption keys. Changing the passphrase indirectly changes the encryption of the keys, but does not affect user data or the underlying encryption key.

Changing the passphrase requires two-user authentication to protect against data shredding.

Procedure

1. Select **System Settings** > **Access Management** > **Administrator Access**.
2. To change the system passphrase, click **Change Passphrase**.

The Change Passphrase dialog appears.

Note

The file system must be disabled to change the passphrase. If the file system is running, you are prompted to disable it.

3. In the text fields, provide:
 - The user name and password of a Security Officer account (an authorized user in the Security User group on that Data Domain system).
 - The current passphrase when changing the passphrase.
 - The new passphrase, which must contain the minimum number of characters configured with the `system passphrase option set min-length` command.
4. Click the checkbox for **Enable file system now**.
5. Click **OK**.

NOTICE

Be sure to take care of the passphrase. If the passphrase is lost, you can never unlock the file system and access the data; the data is irrevocably lost.

System access management

System access management features allow you to control system access to users in a local database or in a network directory. Additional controls define different access levels and control which protocols can access the system.

Role-based access control

Role-based access control (RBAC) is an authentication policy that controls which DD System Manager controls and CLI commands a user can access on a system.

For example, users who are assigned the *admin* role can configure and monitor an entire system, while users who are assigned the *user* role are limited to monitoring a system. When logged into DD System Manager, users see only the program features that they are permitted to use based on the role assigned to the user. The following roles are available for administering and managing the DD OS.

admin

An *admin* role user can configure and monitor the entire Data Domain system. Most configuration features and commands are available only to *admin* role users. However, some features and commands require the approval of a *security* role user before a task is completed.

user

The *user* role enables users to monitor systems and change their own password. Users who are assigned the *user* management role can view system status, but they cannot change the system configuration.

security (security officer)

A *security* role user, who may be referred to as a security officer, can manage other security officers, authorize procedures that require security officer approval, and perform all tasks supported for user-role users.

The *security* role is provided to comply with the Write Once Read-Many (WORM) regulation. This regulation requires electronically stored corporate data be kept in an unaltered, original state for purposes such as eDiscovery. EMC Data Domain added auditing and logging capabilities to enhance this feature. As a result of compliance regulations, most command options for administering sensitive operations, such as encryption, Retention Lock Compliance, and archiving now require security officer approval.

In a typical scenario, an *admin* role user issues a command and, if security officer approval is required, the system displays a prompt for approval. To proceed with the original task, the security officer must enter his or her username and password on the same console at which the command was run. If the system recognizes the security officer credentials, the procedure is authorized. If not, a security alert is generated.

The following are some guidelines that apply to security-role users:

- Only the *sysadmin* user (the default user created during the DD OS installation) can create the first security officer, after which the privilege to create security officers is removed from the *sysadmin* user.
- After the first security officer is created, only security officers can create other security officers.
- Creating a security officer does not enable the authorization policy. To enable the authorization policy, a security officer must log in and enable the authorization policy.
- Separation of privilege and duty apply. *admin* role users cannot perform security officer tasks, and security officers cannot perform system configuration tasks.
- During an upgrade, if the system configuration contains security officers, a *sec-off-defaults* permission is created that includes a list of all current security officers.

backup-operator

A *backup-operator* role user can perform all task permitted for *user* role users, create snapshots for MTrees, and import, export, and move tapes between elements in a virtual tape library.

A *backup-operator* role user can also add and delete SSH public keys for non-password-required log ins. (This function is used mostly for automated scripting.) He or she can add, delete, reset and view CLI command aliases, synchronize modified files, and wait for replication to complete on the destination system.

none

The *none* role is for DD Boost authentication and tenant-unit users only. A *none* role user can log in to a Data Domain system and can change his or her password, but cannot monitor, manage, or configure the primary system. When the primary system is partitioned into tenant units, either the *tenant-admin* or the *tenant-user* role is used to define a user's role with respect to a specific tenant unit. The tenant user is first assigned the *none* role to minimize access to the primary system, and then either the *tenant-admin* or the *tenant-user* role is appended to that user.

tenant-admin

A *tenant-admin* role can be appended to the other (non-tenant) roles when the Secure Multi-Tenancy (SMT) feature is enabled. A *tenant-admin* user can configure and monitor a specific tenant unit.

tenant-user

A *tenant-user* role can be appended to the other (non-tenant) roles when the SMT feature is enabled. The *tenant-user* role enables a user to monitor a specific tenant unit and change the user password. Users who are assigned the *tenant-user* management role can view tenant unit status, but they cannot change the tenant unit configuration.

Access management for IP protocols

This feature manages system access for the FTP, FTPS, HTTP, HTTPS, SSH, SCP, and Telnet protocols.

Viewing the IP services configuration

The Administrator Access tab displays the configuration status for the IP protocols that can be used to access the system. FTP and FTPS are the only protocols that are restricted to administrators.

Procedure

1. In the Navigation panel, select a system.
2. Select **System Settings** > **Access Management**.

Results

The Access Management page displays the Administrator Access, Local Users, and Authentication tabs.

Table 25 Administrator Access tab information

Item	Description
Passphrase	If no passphrase is set, the Set Passphrase button appears. If a passphrase is set, the Change Passphrase button appears.
Services	The name of a service/protocol that can access the system.
Enabled (Yes/No)	The status of the service. If the service is disabled, enable it by selecting it in the list and clicking Configure . Fill out the General tab of the dialog box. If the service is enabled, modify its settings by selecting it in the list and clicking Configure . Edit the settings in the General tab of the dialog box.
Allowed Hosts	The host or hosts that can access the service.
Service Options	The port or session timeout value for the service selected in the list.
<hr/> <p>Note</p> <p>You cannot set options for DD OS 5.2 Data Domain systems that are managed by systems running DD OS 5.3 and later.</p> <hr/>	
FTP/FTPS	Only the session timeout can be set.
HTTP port	The port number opened for the HTTP protocol (port 80, by default).
HTTPS port	The port number opened for the HTTPS protocol (port 443, by default).
SSH/SCP port	The port number opened for the SSH/SCP protocol (port 22, by default).
Telnet	No port number can be set.
Session Timeout	The amount of inactive time allowed before a connection closes. The default is Infinite, that is, the connection does not close. EMC recommends a session timeout maximum of five minutes. Use the Advanced tab of the dialog box to set a timeout in seconds.

Managing FTP access

The File Transfer Protocol (FTP) allows administrators to access files on the Data Domain system.

You can enable either FTP or FTPS access to users who are assigned the admin management role. FTP access allows admin user names and passwords to cross the

network in clear text, making FTP an insecure access method. FTPS is recommended as a secure access method. When you enable either FTP or FTPS access, the other access method is disabled.

Note

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

Note

LFTP clients that connect to a Data Domain system via FTPS or FTP are disconnected after reaching a set timeout limit. However the LFTP client uses its cached username and password to reconnect after the timeout while you are running any command.

Procedure

1. In the Navigation panel, expand **DD Network** and select a managed system.
 2. Select **System Settings > Access Management > Administrator Access**.
 3. Select **FTP** and click **Configure**.
 4. To manage FTP access and which hosts can connect, select the General tab and do the following:
 - a. To enable FTP access, select **Allow FTP Access**.
 - b. To enable all hosts to connect, select **Allow all hosts to connect**.
 - c. To restrict access to select hosts, select **Limit Access to the following systems**, and do the following as needed:
-

Note

You can identify a host using a fully qualified hostname, an IPv4 address, or an IPv6 address.

- To add a host, click Add (+). Enter the host identification and click **OK**.
 - To modify a host ID, select the host in the **Hosts** list and click Edit (pencil). Change the host ID and click **OK**.
 - To remove a host ID, select the host in the **Hosts** list and click Remove (-).
5. To set a session timeout, select the Advanced tab, and enter the timeout value in seconds.
-

Note

The session timeout default is Infinite, that is, the connection does not close.

6. Click **OK**.

If FTPS is enabled, a warning message appears with a prompt to click **OK** to proceed.

Managing FTPS access

The FTP Secure (FTPS) protocol allows administrators to access files on the Data Domain system.

FTPS provides additional security over using FTP, such as support for the Transport Layer Security (TLS) and for the Secure Sockets Layer (SSL) cryptographic protocols. Consider the following guidelines when using FTPS.

- Only users who are assigned the admin management role are permitted to access the system using FTPS.
- When you enable FTPS access, FTP access is disabled.
- FTPS does not show up as a service for DD systems that run DD OS 5.2, managed from a DD system running DD OS 5.3 or later.
- When you issue the `get` command, the fatal error message `SSL_read: wrong version number lftp` appears if matching versions of SSL are not installed on the Data Domain system and compiled on the LFTP client. As a workaround, attempt to re-issue the `get` command on the same file.

Procedure

1. In the Navigation panel, expand **DD Network** and select a managed system.
2. Select **System Settings** > **Access Management** > **Administrator Access**.
3. Select **FTPS** and click **Configure**.
4. To manage FTPS access and which hosts can connect, select the General tab and do the following:
 - a. To enable FTPS access, select **Allow FTPS Access**.
 - b. To enable all hosts to connect, select **Allow all hosts to connect**.
 - c. To restrict access to select hosts, select **Limit Access to the following systems**, and do the following as needed:

Note

You can identify a host using a fully qualified hostname, an IPv4 address, or an IPv6 address.

- To add a host, click Add (+). Enter the host identification and click **OK**.
 - To modify a host ID, select the host in the **Hosts** list and click Edit (pencil). Change the host ID and click **OK**.
 - To remove a host ID, select the host in the **Hosts** list and click Remove (-).
5. To set a session timeout, select the Advanced tab and enter the timeout value in seconds.

Note

The session timeout default is Infinite, that is, the connection does not close.

6. Click **OK**. If FTP is enabled, a warning message appears and prompts you to click **OK** to proceed.

Managing HTTP and HTTPS access

HTTP or HTTPS access is required to support browser access to DD System Manager.

Procedure

1. In the Navigation panel, expand **DD Network** and select a managed system.
2. Select **System Settings** > **Access Management** > **Administrator Access**.
3. Select **HTTP and/or HTTPS** and click **Configure**.

The Configure HTTP/HTTPS Access dialog appears and displays tabs for general configuration, advanced configuration, and certificate management.

4. To manage the access method and which hosts can connect, select the General tab and do the following:
 - a. Select the checkboxes for the access methods you want to allow.
 - b. To enable all hosts to connect, select **Allow all hosts to connect**.
 - c. To restrict access to select hosts, select **Limit Access to the following systems**, and do the following as needed:

Note

You can identify a host using a fully qualified hostname, an IPv4 address, or an IPv6 address.

- To add a host, click Add (+). Enter the host identification and click **OK**.
 - To modify a host ID, select the host in the **Hosts** list and click Edit (pencil). Change the host ID and click **OK**.
 - To remove a host ID, select the host in the **Hosts** list and click Remove (-).
5. To configure system ports and session timeout values, select the Advanced tab, and do the following as needed:
 - In the **HTTP Port** text entry box, enter the port for connection. Port 80 is assigned by default.
 - In the **HTTPS Port** text entry box, enter the port for connection. Port 443 is assigned by default.
 - In the **Session Timeout** text entry box, enter the interval in seconds that must elapse before connection closes. The minimum is 60 seconds and the maximum is 31536000 seconds (one year).

Note

The session timeout default is Infinite, that is, the connection does not close.

6. Click **OK**.

Managing host certificates for HTTP and HTTPS

A host certificate allows browsers to verify the identity of the system when establishing management sessions.

Requesting a host certificate for HTTP and HTTPS

You can use DD System Manager to generate a host certificate request, which you can then forward to a Certificate Authority (CA).

Note

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

Procedure

1. Start DD System Manager on the system to which you want to add a host certificate.

Note

DD System Manager supports certificate management only on the management system (which is the system running DD System Manager).

2. Expand **DD Network** in the Navigation panel and select the management system.
 3. Select **System Settings > Access Management > Administrator Access**.
 4. In the Services area, select **HTTP** or **HTTPS** and click **Configure**.
 5. Select the **Certificate** tab.
-

Note

If you try to remotely manage certificates on a managed system, DD System Manager displays an information message at the top of the certificate management dialog. To manage certificates for a system, you must start DD System Manager on that system.

6. Click **Add**.
A dialog appears for the protocol you selected earlier in this procedure.
 7. Click **Generate the CSR for this Data Domain system**.
The dialog expands to display a CSR form.
-

Note

DD OS supports one active CSR at a time. After a CSR is generated, the **Generate the CSR for this Data Domain system** link is replaced with the **Download the CSR for this Data Domain system** link. To delete a CSR, use the `adminaccess certificate cert-signing-request delete` CLI command.

8. Complete the CSR form and click **Generate and download a CSR**.
The CSR file is saved 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 CA.
-

Adding a host certificate for HTTP and HTTPS

You can use DD System Manager to add a host certificate to the system.

Procedure

1. If you did not request a host certificate, request a host certificate from a certificate authority.
 2. When you receive a host certificate, copy or move it to the computer from which you run DD Service Manager.
 3. Start DD System Manager on the system to which you want to add a host certificate.
-

Note

DD System Manager supports certificate management only on the management system (which is the system running DD System Manager).

4. Expand **DD Network** in the Navigation panel and select the management system.
5. Select **System Settings > Access Management > Administrator Access**.

6. In the Services area, select **HTTP** or **HTTPS** and click **Configure**.
7. Select the **Certificate** tab.

Note

If you try to remotely manage certificates on a managed system, DD System Manager displays an information message at the top of the certificate management dialog. To manage certificates for a system, you must start DD System Manager on that system.

8. Click **Add**.

A dialog appears for the protocol you selected earlier in this procedure.

9. To add a host certificate enclosed in a .p12 file, do the following:
 - a. Select **I want to upload the certificate as a .p12 file**.
 - b. Type the password in the **Password** box.
 - c. Click **Browse** and select the host certificate file to upload to the system.
 - d. Click **Add**.
10. To add a host certificate enclosed in a .pem file, do the following:
 - a. Select **I want to upload the public key as a .pem file and use a generated private key**.
 - b. Click **Browse** and select the host certificate file to upload to the system.
 - c. Click **Add**.

Deleting a host certificate for HTTP and HTTPS

DD OS supports one host certificate for HTTP and HTTPS. If the system is currently using a host certificate and you want to use a different host certificate, you must delete the current certificate before adding the new certificate.

Procedure

1. Start DD System Manager on the system from which you want to delete a host certificate.

Note

DD System Manager supports certificate management only on the management system (which is the system running DD System Manager).

2. Expand **DD Network** in the Navigation panel and select the management system.
3. Select **System Settings** > **Access Management** > **Administrator Access**.
4. In the Services area, select **HTTP** or **HTTPS** and click **Configure**.
5. Select the **Certificate** tab.

Note

If you try to remotely manage certificates on a managed system, DD System Manager displays an information message at the top of the certificate management dialog. To manage certificates for a system, you must start DD System Manager on that system.

6. Select the certificate you want to delete.

7. Click **Delete**, and click **OK**.

Managing SSH and SCP access

SSH is a secure protocol that enables network access to the system CLI, with or without SCP (secure copy). You can use DD System Manager to enable system access using the SSH protocol. SCP requires SSH, so when SSH is disabled, SCP is automatically disabled.

Note

SCP does not show up as a service for DD systems that run DD OS 5.2, managed from a DD system running DD OS 5.3 or later.

Procedure

1. In the Navigation panel, expand **DD Network** and select a managed system.
2. Select **System Settings** > **Access Management** > **Administrator Access**.
3. Select **SSH** or **SCP**.
4. To manage the access method and which hosts can connect, select the **General** tab and do the following:
 - a. Select the checkboxes for the access methods you want to allow.
 - b. To enable all hosts to connect, select **Allow all hosts to connect**.
 - c. To restrict access to select hosts, select **Limit Access to the following systems**, and do the following as needed.

Note

You can identify a host using a fully qualified hostname, an IPv4 address, or an IPv6 address.

-
- To add a host, click **Add (+)**. Enter the host identification and click **OK**.
 - To modify a host ID, select the host in the **Hosts** list and click **Edit** (pencil). Change the host ID and click **OK**.
 - To remove a host ID, select the host in the **Hosts** list and click **Remove (-)**.
5. To configure system ports and session timeout values, click the **Advanced** tab.
 - In the **SSH/SCP Port** text entry box, enter the port for connection. Port 22 is assigned by default.
 - In the **Session Timeout** text entry box, enter the interval in seconds that must elapse before connection closes.

Note

The session timeout default is Infinite, that is, the connection does not close.

Note

Click **Default** to revert to the default value.

6. Click **OK**.

Managing Telnet access

Telnet is an insecure protocol that enables network access to the system CLI.

Note

Telnet access allows user names and passwords to cross the network in clear text, making Telnet an insecure access method.

Procedure

1. In the Navigation panel, expand **DD Network** and select a managed system.
 2. Select **System Settings** > **Access Management** > **Administrator Access**.
 3. Select **Telnet** and click **Configure**.
 4. To manage Telnet access and which hosts can connect, select the General tab and do the following:
 - a. To enable Telnet access, select **Allow Telnet Access**.
 - b. To enable all hosts to connect, select **Allow all hosts to connect**.
 - c. To restrict access to select hosts, select **Limit Access to the following systems**, and do the following as needed.
-

Note

You can identify a host using a fully qualified hostname, an IPv4 address, or an IPv6 address.

- To add a host, click Add (+). Enter the host identification and click **OK**.
 - To modify a host ID, select the host in the **Hosts** list and click Edit (pencil). Change the host ID and click **OK**.
 - To remove a host ID, select the host in the **Hosts** list and click Remove (-).
5. To set a session timeout, select the Advanced tab and enter the timeout value in seconds.
-

Note

The session timeout default is Infinite, that is, the connection does not close.

6. Click **OK**.

Local user account management

A local user is a user account (user name and password) that is configured on the Data Domain system instead of being defined in a Windows Active Directory, Windows Workgroup, or NIS directory.

UID conflicts: local user and NIS user accounts

When you set up a Data Domain system in an NIS environment, be aware of potential UID conflicts between local and NIS user accounts.

Local user accounts on a Data Domain system start with a UID of 500. To avoid conflicts, consider the size of potential local accounts when you define allowable UID ranges for NIS users.

Viewing local user information

Local users are user accounts that are defined on the system, rather than in Active Directory, a Workgroup, or UNIX. You can display the local user's username, management role, login status, and target disable date. You can also display the user's password controls and the tenant units the user can access.

Note

The user-authentication module uses Greenwich Mean Time (GMT). To ensure that user accounts and passwords expire correctly, configure settings to use the GMT that corresponds to the target local time.

Procedure

1. In the Navigation panel, expand the DD Network and select a system.
2. Select **System Settings > Access Management > Local Users** .

The Local Users view appears and shows the Local Users table and the Detailed Information area.

Table 26 Local user list column label descriptions

Item	Description
Name	The user ID, as added to the system.
Management Role	The role displayed is admin, user, security, backup-operator, or none. The tenant user roles do not appear in this table. Tenant user roles are displayed as <i>none</i> . To see an assigned tenant role, select the user and view the role in the Detailed Information area.
Status	<ul style="list-style-type: none"> • Active—User access to the account is permitted. • Disabled—User access to the account is denied because the account is administratively disabled, the current date is beyond the expiration date for the account, or a locked account's password requires renewal. • Locked—User access to the account is denied because the password expired.
Disable Date	The date the account is set to be disabled.
Last Login From	The location where the user last logged in.
Last Login Time	The time the user last logged in.

Note

User accounts configured with the admin or security officer roles can view all users. Users with other roles can view only their own user accounts.

3. Select the user you want to view from the list of users.

Information about the selected user displays in the Detailed Information area.

Table 27 Detailed User Information, Row Label Descriptions

Item	Description
Tenant-User	The list of tenant units the user can access as a tenant-user role user.
Tenant-Admin	The list of tenant units the user can access as a tenant-admin role user.
Password Last Changed	The date the password was last changed.
Minimum Days Between Change	The minimum number of days between password changes that you allow a user. Default is 0.
Maximum Days Between Change	The maximum number of days between password changes that you allow a user. Default is 90.
Warn Days Before Expire	The number of days to warn the users before their password expires. Default is 7.
Disable Days After Expire	The number of days after a password expires to disable the user account. Default is Never.

Note

The default values are the initial default password policy values. A system administrator (admin role) can change them using the Modify Password Policy task.

Creating local users

Create local users when you want to manage access on the local system instead of through an external directory. Data Domain systems support a maximum of 500 local user accounts.

Procedure

1. In the Navigation panel, expand the DD Network and select a system.
2. Select **System Settings > Access Management > Local Users**.
The Local Users view appears.
3. Click the **Create** button to create a new user.
The Create User dialog box appears.
4. Enter user information in the General Tab.

Table 28 Create User dialog, general controls

Item	Description
User	The user ID or name.
Password	The user password. Set a default password, and the user can change it later.
Verify Password	The user password, again.
Role	The role assigned to the user, which can be admin, user, security, backup-operator, or none. .

Table 28 Create User dialog, general controls (continued)

Item	Description
	<p>Note</p> <p>Only the sysadmin user (the default user created during the DD OS installation) can create the first security-role user. After the first security-role user is created, only security-role users can create other security-role users.</p>

The default value for the minimum length of a password is 6 characters. The default value for the minimum number of character classes required for a user password is 1. Allowable character classes include:

- Lowercase letters (a-z)
- Uppercase letters (A-Z)
- Numbers (0-9)
- Special Characters (\$, %, #, +, and so on)

Note

Sysadmin is the default admin-role user and cannot be deleted or modified.

5. To manage password and account expiration, select the Advanced tab and use the controls described in the following table.

Table 29 Create User dialog, advanced controls

Item	Description
Minimum Days Between Change	The minimum number of days between password changes that you allow a user. Default is 0.
Maximum Days Between Change	The maximum number of days between password changes that you allow a user. Default is 90.
Warn Days Before Expire	The number of days to warn the users before their password expires. Default is 7.
Disable Days After Expire	The number of days after a password expires to disable the user account. Default is Never.
Disable account on the following date	Check this box and enter a date (mm/dd/yyyy) when you want to disable this account. Also, you can click the calendar to select a date.

6. Click **OK**.

Note

Note: The default password policy can change if an admin-role user changes them from the Modify Password Policy task. The default values are the initial default password policy values.

Modifying a local user profile

After you create a user, you can use DD System Manager to modify the user configuration.

Procedure

1. In the Navigation panel, expand the DD Network and select a system.
2. Select **System Settings** > **Access Management** > **Local Users**.

The Local Users view appears.

3. Click a user name from the list.
4. Click **Modify** to make changes to a user account.

The Modify User dialog box appears.

5. Update the information on the General tab.

Table 30 Modify User dialog, general controls

Item	Description
User	The user ID or name.
Role	Select the role from the list.

6. Update the information on the Advanced tab.

Table 31 Modify User dialog, advanced controls

Item	Description
Minimum Days Between Change	The minimum number of days between password changes that you allow a user. Default is 0.
Maximum Days Between Change	The maximum number of days between password changes that you allow a user. Default is 90.
Warn Days Before Expire	The number of days to warn the users before their password expires. Default is 7.
Disable Days After Expire	The number of days after a password expires to disable the user account. Default is Never.

7. Click **OK**.

Deleting a local user

You can delete certain users based on your user role. If one of the selected users cannot be deleted, the Delete button is disabled.

The sysadmin user cannot be deleted. Admin users cannot delete security officers. Only security officers can delete, enable, and disable other security officers.

Procedure

1. In the Navigation panel, expand the DD Network and select a system.
2. Select **System Settings** > **Access Management** > **Local Users**.

The Local Users view appears.

3. Click one or more user names from the list.
4. Click **Delete** to delete the user accounts.
The Delete User dialog box appears.
5. Click **OK** and **Close**.

Enabling and disabling local users

Admin users can enable or disable all users except the sysadmin user and users with the security role. The sysadmin user cannot be disabled. Only Security officers can enable or disable other security officers.

Procedure

1. In the Navigation panel, expand the DD Network and select a system.
2. Select **System Settings > Access Management > Local Users**.
The Local Users view appears.
3. Click one or more user names from the list.
4. Click either **Enable** or **Disable** to enable or disable user accounts.
The Enable or Disable User dialog box appears.
5. Click **OK** and **Close**.

Enabling security authorization

You can use the Data Domain system command-line interface (CLI) to enable and disable the security authorization policy.

For information on the commands used in this procedure, see the *EMC Data Domain Operating System Command Reference Guide*.

Note

The Retention Lock Compliance license must be installed. You are not permitted to disable the authorization policy on Retention Lock Compliance systems.

Procedure

1. Log into the CLI using a security officer username and password.
2. To enable the security officer authorization policy, enter: `# authorization policy set security-officer enabled`

Changing user passwords

After you create a user, you can use DD System Manager to change the user's password. Individual users can also change their own passwords.

Procedure

1. In the Navigation panel, expand the DD Network and select a system.
2. Click **System Settings > Access Management > Local Users**.
The Local Users view appears.
3. Click a user name from the list.
4. Click **Change Password** to change the user password.
The Change Password dialog box appears.

If prompted, enter your old password.

5. Enter the new password into the **New Password** box.
6. Enter the new password again into **Verify New Password** box.
7. Click **OK**.

Modifying the password policy and login controls

The password policy and login controls define login requirements for all users. Administrators can specify how often a password must be changed, what is required to create a valid password, and how the system responds to invalid login attempts.

Procedure

1. In the Navigation panel, expand **DD Network** and select a managed system.
2. Select **System Settings > Access Management**.
3. Select **More Tasks > Change Login Options**.
The Change Login Options dialog appears.
4. Specify the new configuration in the boxes for each option. To select the default value, click **Default** next to the appropriate option.
5. Click **OK** to save the password settings.

Change Login Options dialog

Use this dialog to set the password policy and specify the maximum login attempts and lockout period.

Table 32 Change Login Options dialog controls

Item	Description
Minimum Days Between Change	The minimum number of days between password changes that you allow a user. This value must be less than the Maximum Days Between Change value minus the Warn Days Before Expire value. The default setting is 0.
Maximum Days Between Change	The maximum number of days between password changes that you allow a user. The minimum value is 1. The default value is 90.
Warn Days Before Expire	The number of days to warn the users before their password expires. This value must be less than the Maximum Days Between Change value minus the Minimum Days Between Change value. The default setting is 7.
Disable Days After Expire	The system disables a user account after password expiration according to the number of days specified with this option. Valid entries are <i>never</i> or number greater than or equal to 0. The default setting is never.
Minimum Length of Password	The minimum password length required. Default is 6.
Minimum Number of Character Classes	The minimum number of character classes required for a user password. Default is 1. Character classes include: <ul style="list-style-type: none"> • Lowercase letters (a-z) • Uppercase letters (A-Z)

Table 32 Change Login Options dialog controls (continued)

Item	Description
	<ul style="list-style-type: none"> Numbers (0-9) Special Characters (\$, %, #, +, and so on)
Lowercase Character Requirement	Enable or disable the requirement for at least one lowercase character. The default setting is disabled.
Uppercase Character Requirement	Enable or disable the requirement for at least one uppercase character. The default setting is disabled.
One Digit Requirement	Enable or disable the requirement for at least one numerical character. The default setting is disabled.
Special Character Requirement	Enable or disable the requirement for at least one special character. The default setting is disabled.
Max Consecutive Character Requirement	Enable or disable the requirement for a maximum of three repeated characters. The default setting is disabled.
Prevent use of Last N Passwords	Specify the number of remembered passwords. The range is 0 to 24, and the default settings is 1.
	<p>Note</p> <p>If this setting is reduced, the remembered password list remains unchanged until the next time the password is changed. For example, if this setting is changed from 4 to 3, the last four passwords are remembered until the next time the password is changed.</p>
Maximum login attempts	Specifies the maximum number of login attempts before a mandatory lock is applied to a user account. This limit applies to all user accounts, including sysadmin. A locked user cannot log in while the account is locked. The range is 4 to 20, and the default value is 4.
Unlock timeout (seconds)	Specifies how long a user account is locked after the maximum number of login attempts. When the configured unlock timeout is reached, a user can attempt login. The range is 120 to 3600 seconds, and the default period is 120 seconds.

Directory user and group management

You can use DD System manager to manage access to the system for users and groups in Windows Active Directory, Windows Workgroup, and NIS. Kerberos authentication is an option for CIFS and NFS clients.

Viewing Active Directory and Kerberos information

The Active Directory Kerberos configuration determines the methods CIFS and NFS clients use to authenticate. The Active Directory/Kerberos Authentication panel displays this configuration.

Procedure

1. In the Navigation panel, expand **DD Network** and select a managed system.
2. Select **System Settings > Access Management > Authentication**.

3. Expand the Active Directory/Kerberos Authentication panel.

Table 33 Active Directory/ Kerberos Authentication label descriptions

Item	Description
Mode	The type of authentication mode. In Windows/Active Directory mode, CIFS clients use Active Directory and Kerberos authentication, and NFS clients use Kerberos authentication. In Unix mode, CIFS clients use Workgroup authentication (without Kerberos), and NFS clients use Kerberos authentication. In Disabled mode, Kerberos authentication is disabled and CIFS clients use Workgroup authentication.
Realm	The realm name of the Workgroup or Active Directory.
DDNS	Whether or not the Dynamic Domain Name System is enabled.
Domain Controllers	The name of the domain controller for the Workgroup or Active Directory.
Organizational Unit	The name of the organizations unit for the Workgroup or Active Directory.
CIFS Server Name	The name of the CIFS server in use (Windows mode only).
WINS Server	The name of the WINS server in use (Windows mode only).
Short Domain Name	An abbreviated name for the domain.
NTP	Enabled/Disabled (UNIX mode only)
NIS	Enabled/Disabled (UNIX mode only)
Key Distribution Centers	Hostname(s) or IP(s) of KDC in use (UNIX mode only)
Active Directory Administrative Access	Enabled/Disabled: Click to Enable or disable administrative access for Active Directory (Windows) groups.

Table 34 Active Directory administrative groups and roles

Item	Description
Windows Group	The name of the Windows group.
Management Role	The role of the group (admin, user, and so on)

Configuring Active Directory and Kerberos authentication

Configuring Active Directory authentication makes the Data Domain system part of a Windows Active Directory realm. CIFS clients and NFS clients use Kerberos authentication.

Procedure

1. In the Navigation panel, expand the DD Network and select a system.
2. Select **System Settings > Access Management > Authentication**.
The Authentication view appears.
3. Expand the Active Directory/Kerberos Authentication panel.
4. Click **Configure...** next to Mode to start the configuration wizard.

The Active Directory/Kerberos Authentication dialog appears.

5. Select **Windows/Active Directory** and click **Next**.
6. Enter the full realm name for the system (for example: domain1.local), the user name, and password for the Data Domain system. Then click **Next**.

Note

Use the complete realm name. Ensure that the user is assigned sufficient privileges to join the system to the domain. The user name and password must be compatible with Microsoft requirements for the Active Directory domain. This user must also be assigned permission to create accounts in this domain.

7. Select the default CIFS server name, or select **Manual** and enter a CIFS server name.
8. To select domain controllers, select **Automatically assign**, or select **Manual** and enter up to three domain controller names.
You can enter fully qualified domain names, hostnames, or IP (IPv4 or IPv6) addresses.
9. To select an organizational unit, select **Use default Computers**, or select **Manual** and enter an organization unit name.

Note

The account is moved to the new organizational unit.

10. Click **Next**.
The Summary page for the configuration appears.
11. Click **Finish**.
The system displays the configuration information in the Authentication view.
12. To enable administrative access, click **Enable** to the right of **Active Directory Administrative Access**.

Authentication mode selections

The authentication mode selection determines how CIFS and NFS clients authenticate using supported combinations of Active Directory, Workgroup, and Kerberos authentication.

DD OS supports the following authentication options.

- **Disabled:** Kerberos authentication is disabled for CIFS and NFS clients. CIFS clients use Workgroup authentication.
- **Windows/Active Directory:** Kerberos authentication is enabled for CIFS and NFS clients. CIFS clients use Active Directory authentication.
- **Unix:** Kerberos authentication is enabled for only NFS clients. CIFS clients use Workgroup authentication.

Managing administrative groups for Active Directory

You can use the Active Directory/Kerberos Authentication panel to create, modify, and delete Active Directory (Windows) groups and assign management roles (admin, backup-operator, and so on) to those groups.

To prepare for managing groups, select **System Settings > Access Management > Authentication**, expand the Active Directory/Kerberos Authentication panel, and click the Active Directory Administrative Access **Enable** button.

Creating administrative groups for Active Directory

Create an administrative group when you want to assign a management role to all the users configured in an Active Directory group.

Before you begin

Enable Active Directory Administrative Access on the Active Directory/Kerberos Authentication panel in the **System Settings > Access Management > Authentication** page.

Procedure

1. Click **Create....**
2. Enter the domain and group name separated by a backslash. For example: domainname\groupname.
3. Select the management role for the group from the drop-down menu.
4. Click **OK**.

Modifying administrative groups for Active Directory

Modify an administrative group when you want to change the administrative group name or management role configured for an Active Directory group.

Before you begin

Enable Active Directory Administrative Access on the Active Directory/Kerberos Authentication panel in the **System Settings > Access Management > Authentication** page.

Procedure

1. Select a group to modify under the **Active Directory Administrative Access** heading.
2. Click **Modify....**
3. Modify the domain and group name. These names are separated by a backslash. For example: domainname\groupname.
4. Modify the management role for the group by selecting a different role from the drop-down menu.

Deleting administrative groups for Active Directory

Delete an administrative group when you want to terminate system access for all the users configured in an Active Directory group.

Before you begin

Enable Active Directory Administrative Access on the Active Directory/Kerberos Authentication panel in the **System Settings > Access Management > Authentication** page.

Procedure

1. Select a group to delete under the **Active Directory Administrative Access** heading.
2. Click **Delete**.

Configuring UNIX Kerberos authentication

Configuring UNIX Kerberos authentication enables NFS clients to use Kerberos authentication. CIFS clients use Workgroup authentication.

Before you begin

NIS must be running for UNIX-mode Kerberos authentication to function. For instructions about enabling Kerberos, see the section regarding enabling NIS services.

Configuring Kerberos for UNIX enables NFS clients to use Kerberos authentication. CIFS clients use Workgroup authentication.

Procedure

1. In the Navigation panel, expand the DD Network and select a system.
2. Select **System Settings** > **Access Management** > **Authentication**.

The Authentication view appears.

3. Expand the Active Directory/Kerberos Authentication panel.
4. Click **Configure...** next to Mode to start the configuration wizard.

The Active Directory/Kerberos Authentication dialog appears.

5. Select **Unix** and click **Next**.
6. Enter the realm name (for example: domain1.local), and up to three host names or IP addresses (IPv4 or IPv6) for key distribution centers (KDCs).
7. Optionally, click **Browse** to upload a keytab file, and click **Next**.

The Summary page for the configuration appears.

Note

Keytab files are generated on the authentication servers (KDCs) and contain a shared secret between the KDC server and the DDR.

NOTICE

A keytab file must be uploaded and imported for Kerberos authentication to operate correctly.

8. Click **Finish**.

The system displays the configuration information in the Active Directory/Kerberos Authentication panel.

Disabling Kerberos authentication

Disabling Kerberos authentication prevents CIFS and NFS clients from using Kerberos authentication. CIFS clients use Workgroup authentication.

Procedure

1. In the Navigation panel, expand the DD Network and select a system.
2. Select **System Settings** > **Access Management** > **Authentication**.

The Authentication view appears.

3. Expand the Active Directory/Kerberos Authentication panel.
4. Click **Configure...** next to Mode to start the configuration wizard.

The Active Directory/Kerberos Authentication dialog appears.

5. Select **Disabled** and click **Next**.

The system displays a summary page with changes appearing in bold text.

6. Click **Finish**.

The system displays Disabled next to Mode in the Active Directory/Kerberos Authentication panel.

Viewing Workgroup authentication information

Use the Workgroup Authentication panel to view Workgroup configuration information.

Procedure

1. In the Navigation panel, expand **DD Network** and select a managed system.
2. Select **System Settings > Access Management > Authentication**.
3. Expand the Workgroup Authentication panel.

Table 35 Workgroup Authentication label descriptions

Item	Description
Mode	The type of authentication mode (Workgroup or Active Directory).
Workgroup name	The specified workgroup
CIFS Server Name	The name of the CIFS server in use.
WINS Server	The name of the WINS server in use.

Configuring workgroup authentication parameters

Workgroup authentication parameters allow you to configure a Workgroup name and CIFS server name.

Procedure

1. In the Navigation panel, expand the DD Network and select a system.
2. Select **System Settings > Access Management > Authentication**.

The Authentication view appears.

3. Expand the Workgroup Authentication panel.
4. Click **Configure**.

The Workgroup Authentication dialog appears.

5. For Workgroup Name, select **Manual** and enter a workgroup name to join, or use the default.

The Workgroup mode joins a Data Domain system to a workgroup domain.

6. For CIFS Server Name, select **Manual** and enter a server name (the DDR), or use the default.
7. Click **OK**.

Viewing NIS authentication information

The NIS Authentication panel displays the NIS configuration parameters and whether NIS authentication is enabled or disabled.

Procedure

1. In the Navigation panel, expand **DD Network** and select a managed system.
2. Select **System Settings** › **Access Management** › **Authentication**.

The Authentication view appears.

3. Expand the NIS Authentication panel.

Results

Table 36 NIS Authentication panel items

Item	Description
NIS Status	Enabled or Disabled.
Domain Name	The name of the domain for this service.
Server	Authentication server(s).
NIS Group	The name of the NIS group.
Management Role	The role of the group (admin, user, and so on).

Enabling and disabling NIS authentication

Use the NIS Authentication panel to enable and disable NIS authentication.

Procedure

1. In the Navigation panel, expand the DD Network and select a system.
2. Select **System Settings** › **Access Management** › **Authentication**.

The Authentication view appears.

3. Expand the NIS Authentication panel.
4. Click **Enable** next to NIS Status to enable or **Disable** to disable NIS Authentication.

The Enable or Disable NIS dialog box appears.

5. Click **OK**.

Configuring the NIS domain name

Use the NIS Authentication panel to configure the NIS domain name.

Procedure

1. In the Navigation panel, expand the DD Network and select a system.
2. Select **System Settings** › **Access Management** › **Authentication**.

The Authentication view appears.

3. Expand the NIS Authentication panel.
4. Click **Edit** next to Domain Name to edit the NIS domain name.

The Configure NIS Domain Name dialog box appears.

5. Enter the domain name in the **Domain Name** box.
6. Click **OK**.

Specifying NIS authentication servers

Use the NIS Authentication panel to specify NIS authentication servers.

Procedure

1. In the Navigation panel, expand the DD Network and select a system.
2. Select **System Settings** > **Access Management** > **Authentication**.
The Authentication view appears.
3. Expand the NIS Authentication panel.
4. Below Domain Name, select one of the following:
 - **Obtain NIS Servers from DHCP** The system automatically obtains NIS servers using DHCP
 - **Manually Configure** Use the following procedures to manually configure NIS servers.
 - To add an authentication server, click Add (+) in the server table, enter the server name, and click **OK**.
 - To modify an authentication server, select the authentication server name and click the edit icon (pencil). Change the server name, and click **OK**.
 - To remove an authentication server name, select a server, click the X icon, and click **OK**.
5. Click **OK**.

Configuring NIS groups

Use the NIS Authentication panel to configure NIS groups.

Procedure

1. In the Navigation panel, expand the DD Network and select a system.
2. Select **System Settings** > **Access Management** > **Authentication**.
The Authentication view appears.
3. Expand the NIS Authentication panel.
4. Configure the NIS groups in the NIS Group table.
 - To add a NIS group, click Add (+), enter the NIS group name and role, and click **Validate**. Click **OK** to exit the add NIS group dialog box. Click **OK** again to exit the **Configure Allowed NIS Groups** dialog box.
 - To modify an NIS group, select the checkbox of the NIS group name in the NIS group list and click Edit (pencil). Change the NIS group name, and click **OK**.
 - To remove an NIS group name, select the NIS group in the list and click Delete **X**.
5. Click **OK**.

Configuring mail server settings

The Mail Server tab allows you to specify the mail server to which DD OS sends email reports.

Procedure

1. Select **System Settings** > **General Configuration** > **Mail Server**.
2. Select **More Tasks** > **Set Mail Server**.

The Set Mail Server dialog box appears.

3. Enter the name of the mail server in the **Mail Server** box.
4. Click **OK**.

Managing time and date settings

The Time and Date Settings tab allows you to view and configure the system time and date or configure the Network Time Protocol to set the time and date.

Procedure

1. To view the current time and date configuration, select **System Settings** > **General Configuration** > **Time and Date Settings**.

The Time and Date Settings page presents the current system date and time, shows whether NTP is enabled or not, and lists the IP addresses or hostnames of configured NTP servers.

2. To change the configuration, select **More Tasks** > **Configure Time Settings**.

The Configure Time Settings dialog appears.

3. In the **Time Zone** dropdown list, select the time zone where the Data Domain system resides.
4. To manually set the time and date, select **None**, type the date in the **Date** box, and select the time in the **Time** dropdown lists.
5. To use NTP to synchronize the time, select NTP and set how the NTP server is accessed.
 - **Obtain NTP Servers using DHCP.**
 - **Manually Configure.** add the IP address of the server, and click **OK**.

Note

Using time synchronization from an Active Directory domain controller might cause excessive time changes on the system if both NTP and the domain controller are modifying the time.

6. Click **OK**.
7. If you changed the time zone, you must reboot the system.

- a. Select **Maintenance** › **System**.
- b. From the More Tasks menu, select Reboot System.
- c. Click OK to confirm.

Managing system properties

The System Properties tab allows you to view and configure system properties that identify the managed system location, administrator email address, and host name.

Procedure

1. In the Navigation panel, expand **DD Network** and select a managed system.
2. To view the current configuration, select **System Settings** › **General Configuration** › **System Properties**.

The System Properties tab displays the system location, the administrator email address, and the administrator hostname.

3. To change the configuration, select **More Tasks** › **Set System Properties**.

The Set System Properties dialog box appears.

4. In the **Location** box, enter information about where the Data Domain system is located.
5. In the **Admin Email** box, enter the email address of the system administrator.
6. In the **Admin Host** box, enter the name of the administration server.
7. Click **OK**.

SNMP management

The Simple Network Management Protocol (SNMP) is a standard protocol for exchanging network management information, and is a part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP provides a tool for network administrators to manage and monitor network-attached devices, such as Data Domain systems, for conditions that warrant administrator attention.

To monitor Data Domain systems using SNMP, you will need to install the Data Domain MIB in your SNMP Management system. DD OS also supports the standard MIB-II so you can also query MIB-II statistics for general data such as network statistics. For full coverage of available data you should utilize both the Data Domain MIB and the standard MIB-II MIB.

The Data Domain system SNMP agent accepts queries for Data Domain-specific information from management systems using SNMP v1, v2c, and v3. SNMP V3 provides a greater degree of security than v2c and v1 by replacing cleartext community strings (used for authentication) with user-based authentication using either MD5 or SHA1. Also, SNMP v3 user authentication packets can be encrypted and their integrity verified with either DES or AES.

Data Domain systems can send SNMP traps (which are alert messages) using SNMP v2c and SNMP v3. Because SNMP v1 traps are not supported, EMC recommends using SNMP v2c or v3.

The default port that is open when SNMP is enabled is port 161. Traps are sent out through port 162.

- The *EMC Data Domain Operating System Initial Configuration Guide* describes how to set up the Data Domain system to use SNMP monitoring.
- The *EMC Data Domain Operating System MIB Quick Reference* describes the full set of MIB parameters included in the Data Domain MIB branch.

Viewing SNMP status and configuration

The SNMP tab displays the current SNMP status and configuration.

Procedure

1. Select the system to be checked in the Navigation panel.
2. Select **System Settings > General Configuration > SNMP**.

The SNMP view shows the SNMP status, SNMP properties, SNMP V3 configuration, and SNMP V2C configuration.

SNMP tab labels

The SNMP tab labels identify the overall SNMP status, SNMP property values, and the configurations for SNMPv3 and SNMPv2.

Status

The Status area displays the operational status of the SNMP agent on the system, which is either Enabled or Disabled.

SNMP Properties

Table 37 SNMP Properties descriptions

Item	Description
SNMP System Location	The location of the Data Domain system being monitored.
SNMP System Contact	The person designated as the person to contact for the Data Domain system administration.

SNMP V3 Configuration

Table 38 SNMP Users column descriptions

Item	Description
Name	The name of the user on the SNMP manager with access to the agent for the Data Domain system.
Access	The access permissions for the SNMP user, which can be Read-only or Read-write.
Authentication Protocols	The Authentication Protocol used to validate the SNMP user, which can be MD5, SHA1, or None.
Privacy Protocol	The encryption protocol used during the SNMP user authentication, which can be AES, DES, or None.

Table 39 Trap Hosts column descriptions

Item	Description
Host	The IP address or domain name of the SNMP management host.
Port	The port used for SNMP trap communication with the host. For example, 162 is the default.
User	The user on the trap host authenticated to access the Data Domain SNMP information.

SNMP V2C Configuration

Table 40 Communities column descriptions

Item	Description
Community	The name of the community. For example, public, private, or localCommunity.
Access	The access permission assigned, which can be Read-only or Read-write.
Hosts	The hosts in this community.

Table 41 Trap Hosts column descriptions

Item	Description
Host	The systems designated to receive SNMP traps generated by the Data Domain system. If this parameter is set, systems receive alert messages, even if the SNMP agent is disabled.
Port	The port used for SNMP trap communication with the host. For example, 162 is the default.
Community	The name of the community. For example, public, private, or localCommunity.

Enabling and disabling SNMP

Use the SNMP tab to enable or disable SNMP.

Procedure

1. From the **System Settings > General Configuration** page, click **SNMP**.
2. In the Status area, click **Enable** or **Disable**.

Downloading the SNMP MIB

Use the SNMP tab to download the SNMP MIB.

Procedure

1. From the **System Settings > General Configuration > SNMP** page, click **Download MIB file**.
2. In the Opening DATA_DOMAIN.mib dialog box, select **Open**.

3. Click **Browse** and select a browser to view the MIB in a browser window.

Note

If using the Microsoft Internet Explorer browser, enable Automatic prompting for file download.

4. Save the MIB or exit the browser.

Configuring SNMP properties

Use the SNMP tab to configure the text entries for system location and system contact.

Procedure

1. From the **System Settings > General Configuration** page, click **SNMP**.
2. In the SNMP Properties area, click **Configure**.
The SNMP Configuration dialog box appears.
3. In the text fields, add an SNMP system location (a description of where the Data Domain system is located) and/or an SNMP system contact (for example, the email address of the system administrator for the Data Domain system).
4. Click **OK**.

SNMP V3 user management

Use the SNMP tab to create, modify, and delete SNMPv3 users and trap hosts.

Creating SNMP V3 users

When you create SNMPv3 users, you define a username, specify either read-only or read-write access, and select an authentication protocol.

Procedure

1. From the **System Settings > General Configuration** page, click **SNMP**.
2. In the SNMP Users area, click **Create**.
The Create SNMP User dialog box appears.
3. In the **Name** text field, enter the name of the user for whom you want to grant access to the Data Domain system agent. The name must be a minimum of eight characters.
4. Select either read-only or read-write access for this user.
5. To authenticate the user, select **Authentication**.
 - a. Select either the MD5 or the SHA1 protocol.
 - b. Enter the authentication key in the **Key** text field.
 - c. To provide encryption to the authentication session, select **Privacy**.
 - d. Select either the AES or the DES protocol.
 - e. Enter the encryption key in the **Key** text field.
6. Click **OK**.

The newly added user account appears in the SNMP Users table.

Modifying SNMP V3 users

You can modify the access level (read-only or read-write) and authentication protocol for existing SNMPv3 users.

Procedure

1. From the **System Settings > General Configuration** page, click **SNMP**.
2. In the **SNMP Users** area, select a checkbox for the user and click **Modify**.

The Modify SNMP User dialog box appears. Add or change any of the following settings.

3. Select either read-only or read-write access for this user.
4. To authenticate the user, select **Authentication**.
 - a. Select either the MD5 or the SHA1 protocol.
 - b. Enter the authentication key in the Key text field.
 - c. To provide encryption to the authentication session, select **Privacy**.
 - d. Select either the AES or the DES protocol.
 - e. Enter the encryption key in the **Key** text field.
5. Click **OK**.

The new settings for this user account appear in the SNMP Users table.

Removing SNMP V3 users

Use the SNMP tab to delete existing SNMPv3 users.

Procedure

1. From the **System Settings > General Configuration** page, click **SNMP**.
2. In the SNMP Users area, select a checkbox for the user and click **Delete**.

The Delete SNMP User dialog box appears.

Note

If the **Delete** button is disabled, the selected user is being used by one or more trap hosts. Delete the trap hosts and then delete the user.

3. Verify the user name to be deleted and click **OK**.
4. In the Delete SNMP User Status dialog box, click **Close**.

The user account is removed from the SNMP Users table.

SNMP V2C community management

Define SNMP v2c communities (which serve as passwords) to control management system access to the Data Domain system. To restrict access to specific hosts that use the specified community, assign the hosts to the community.

Note

The SNMP V2c Community string is sent in cleartext and is very easy to intercept. If this occurs, the interceptor can retrieve information from devices on your network, modify their configuration, and possibly shut them down. SNMP V3 provides authentication and encryption features to prevent interception.

Note

SNMP community definitions do not enable the transmission of SNMP traps to a management station. You must define trap hosts to enable trap submission to management stations.

Creating SNMP V2C communities

Create communities to restrict access to the DDR system or for use in sending traps to a trap host. You must create a community and assign it to a host before you can select that community for use with the trap host.

Procedure

1. Select **System Settings** > **General Configuration** > **SNMP**.
2. In the Communities area, click **Create**.
The Create SNMP V2C Community dialog box appears.
3. In the **Community** box, enter the name of a community for whom you want to grant access to the Data Domain system agent.
4. Select either read-only or read-write access for this community.
5. If you want to associate the community to one or more hosts, add the hosts as follows:
 - a. Click **+** to add a host.
The Host dialog box appears.
 - b. In the **Host** text field, enter the IP address or domain name of the host.
 - c. Click **OK**.
The Host is added to the host list.
6. Click **OK**.
The new community entry appears in the **Communities** table and lists the selected hosts.

Modifying SNMP V2C communities

You can modify the access level (read-only or read-write) and host list for existing SNMPv2 communities.

Procedure

1. From the **System Settings > General Configuration** page, click **SNMP**.
2. In the Communities area, select the checkbox for the community and click **Modify**.

The Modify SNMP V2C Community dialog box appears.

Note

The **Modify** button for the selected community is disabled when a trap host on the same system is configured as part of that community. To modify the access setting, delete the trap host and add it back after the community is modified.

Note

The **Modify** button for the selected community is not disabled when the trap host uses an IPv6 address and the system is managed by an earlier DD OS version that does not support IPv6. EMC recommends that you always select a management system that uses the same or a newer DD OS version than the systems it manages.

3. To change the access mode for this community, select either **read-only** or **read-write** access.
 4. To add one or more hosts to this community, do the following:
 - a. Click **+** to add a host.
The Host dialog box appears.
 - b. In the **Host** text field, enter the IP address or domain name of the host.
 - c. Click **OK**.
The Host is added to the host list.
 5. To delete one or more hosts from the host list, do the following:
-

Note

DD System Manager does not allow you to delete a host when a trap host on the same system is configured as part of that community. To delete a trap host from a community, delete the trap host and add it back after the community is modified.

- a. Select the checkbox for each host or click the Host check box in the table head to select all listed hosts.
 - b. Click the delete button (X).
6. To edit a host name, do the following:
 - a. Select the checkbox for the host.
 - b. Click the edit button (pencil icon).
 - c. Edit the host name.
 - d. Click **OK**.

7. Click **OK**.

The modified community entry appears in the Communities table.

Deleting SNMP V2C communities

Use the SNMP tab to delete existing SNMPv2 communities.

Procedure

1. From the **System Settings > General Configuration** page, click **SNMP**.
2. In the **Communities** area, select a checkbox for the community and click **Delete**.

The Delete SNMP V2C Communities dialog box appears.

Note

If the **Delete** button is disabled, the selected community is being used by one or more trap hosts. Delete the trap hosts and then delete the community.

3. Verify the community name to be deleted and click **OK**.
4. In the Delete SNMP V2C Communities Status dialog box, click **Close**. The community entry is removed from the Communities table.

SNMP trap host management

Trap host definitions enable Data Domain systems to send alert messages in SNMP trap messages to an SNMP management station.

Creating SNMP V3 and V2C trap hosts

Trap host definitions identify remote hosts that receive SNMP trap messages from the system.

Before you begin

If you plan to assign an existing SNMP v2c community to a trap host, you must first use the Communities area to assign the trap host to the community.

Procedure

1. From the **System Settings > General Configuration** page, click **SNMP**.
2. In the SNMP V3 Trap Hosts or SNMP V2C Trap Hosts area, click **Create**.
The Create SNMP [V3 or V2C] Trap Hosts dialog appears.
3. In the **Host** box, enter the IP address or domain name of the SNMP Host to receive traps.
4. In the **Port** box, enter the port number for sending traps (port 162 is a common port).
5. Select the user (SNMP V3) or the community (SNMP V2C) from the drop-down menu.

Note

The Community list displays only those communities to which the trap host is already assigned.

6. To create a new community, do the following:

- a. Select **Create New Community** in the Community drop-down menu.
 - b. Enter the name for the new community in the **Community** box.
 - c. Select the Access type.
 - d. Click the add (+) button.
 - e. Enter the trap host name.
 - f. Click **OK**.
 - g. Click **OK**.
7. Click **OK**.

Modifying SNMP V3 and V2C trap hosts

You can modify the port number and community selection for existing trap host configurations.

Procedure

1. From the **System Settings > General Configuration** page, click **SNMP**.
2. In the **SNMP V3 Trap Hosts** or **SNMP V2C Trap Hosts** area, select a Trap Host entry, and click **Modify**.

The Modify SNMP [V3 or V2C] Trap Hosts dialog box appears.

3. To modify the port number, enter a new port number in the **Port** box (port 162 is a common port).
4. Select the user (SNMP V3) or the community (SNMP V2C) from the drop-down menu.

Note

The Community list displays only those communities to which the trap host is already assigned.

5. To create a new community, do the following:
 - a. Select **Create New Community** in the Community drop-down menu.
 - b. Enter the name for the new community in the **Community** box.
 - c. Select the Access type.
 - d. Click the add (+) button.
 - e. Enter the trap host name.
 - f. Click **OK**.
 - g. Click **OK**.
6. Click **OK**.

Removing SNMP V3 and V2C trap hosts

Use the SNMP tab to delete existing trap host configurations.

Procedure

1. From the **System Settings > General Configuration** page, click **SNMP**.
2. In the **Trap Hosts** area (either for V3 or V2C, select a checkbox for the trap host and click **Delete**.

The Delete SNMP [V3 or V2C] Trap Hosts dialog box appears.

3. Verify the host name to be deleted and click **OK**.
4. In the Delete SNMP [V3 or V2C] Trap Hosts Status dialog box, click **Close**.

The trap host entry is removed from the **Trap Hosts** table.

Autosupport report management

The Autosupport feature generates a report called an ASUP. The ASUP shows system identification information, consolidated output from a number of Data Domain system commands, and entries from various log files. Extensive and detailed internal statistics appear at the end of the report. This report is designed to aid EMC Data Domain Support in debugging system problems.

An ASUP is generated every time the file system is started, which is usually once per day. However, the file system can be started more than once in a day.

You can configure email addresses to receive the daily ASUP reports, and you can enable or disable sending of these reports to EMC Data Domain. The default time for sending the daily ASUP is 06.00 a.m, and it is configurable. When sending ASUPs to EMC, you have the option to select the legacy unsecure method or the ConnectEMC method, which encrypts the information before transmission.

Enabling and disabling autosupport reporting to EMC

By default, autosupport reports are enabled and sent daily to EMC Data Domain Customer Support using the legacy email method. The ConnectEMC method sends messages in a secure format using email, FTP, or HTTPS. You can use either method, or you can disable autosupport reporting.

Procedure

1. To view the autosupport reporting status, select **Maintenance** > **Support** > **Autosupport**.

The autosupport notification status is highlighted in green in the Vendor Support area. If ConnectEMC reporting is configured, the selected ConnectEMC mode appears below the Notification Status. Otherwise, the email address for the legacy communication method appears.

2. To display the selected EMC notification method, enter the CLI command: `support notification method show`.
3. To enable autosupport reporting using the legacy method, do the following.
 - a. If ConnectEMC notification is selected, enter the command: `support notification method set email`.
 - b. In DD SM, select **Maintenance** > **Support** > **Autosupport**.
 - c. Select **Enable** in the Vendor Support area.
4. To enable autosupport reporting using ConnectEMC, do the following.

- a. Verify that an administrator email is configured on the system by entering the `config show admin-email` command.

A system administrator email must be configured before you can select the ConnectEMC method.

- b. To configure a system administrator email address, enter the `config set admin-email email-addr` command.

- c. If legacy email notification is selected, enter the command: `support notification method set connectemc.`
 - d. In DD SM, select **Maintenance** › **Support** › **Autosupport**.
 - e. Select **Enable** in the Vendor Support area.
5. To disable autosupport reporting to EMC, do the following.
- a. In DD SM, select **Maintenance** › **Support** › **Autosupport**.
 - b. Select **Disable** in the Vendor Support area.

Reviewing generated autosupport reports

Review autosupport reports to view system statistics and configuration information captured in the past. The system stores a maximum of 14 autosupport reports.

Procedure

1. Select the system to be checked in the Navigation panel.
2. Select **Maintenance** › **Support** › **Autosupport**.

The Autosupport Reports page shows the autosupport report file name and file size, and the date the report was generated. Reports are automatically named. The most current report is autosupport, the previous day is autosupport.1, and the number increments as the reports move back in time.
3. Click the file name link to view the report using a text editor. If doing so is required by your browser, download the file first.

Configuring the autosupport mailing list

Autosupport mailing list subscribers receive autosupport messages through email. Use the Autosupport tab to add, modify, and delete subscribers.

Autosupport emails are sent through the configured mail server to all subscribers in the autosupport email list. After you configure the mail server and autosupport email list, it is a good practice to test the setup to ensure that autosupport messages reach the intended destinations.

Procedure

1. Select **Maintenance** › **Support** › **Autosupport**.
2. Click **Configure**.

The Configure Autosupport Subscribers dialog box appears.
3. To add a subscriber, do the following.
 - a. Click Add (+).

The Email dialog box appears.
 - b. Enter the recipients email address in the Email box.
 - c. Click OK.
4. To delete a subscriber, do the following.
 - a. In the Configure Autosupport Subscribers dialog box, select the subscriber to delete.
 - b. Click Delete (X).

5. To modify a subscriber email address, do the following.
 - a. In the Configure Autosupport Subscribers dialog box, select the subscriber name to edit.
 - b. Click Modify (pencil icon).
The Email dialog box appears.
 - c. Modify the email address as needed.
 - d. Click OK.
6. Click **OK** to close the Configure Autosupport Subscribers dialog box.
The revised autosupport email list appears in the Autosupport Mailing List area.

Support bundle management

A support bundle is a file that contains system configuration and operation information. It is a good practice to generate a support bundle before a software upgrade or a system topology change (such as a controller upgrade).

EMC Data Domain Support often requests a support bundle when providing assistance.

Generating a support bundle

When troubleshooting problems, EMC Data Domain Customer Support may ask for a support bundle, which is a tar-g-zipped selection of log files with a README file that includes identifying autosupport headers.

Procedure

1. Select a managed system in the Navigation panel.
2. Select **Maintenance** > **Support** > **Support Bundles**.
3. Click **Generate Support Bundle**.

Note

The system supports a maximum of 10 support bundles. If you attempt to generate an 11th support bundle, DD System Manager displays a warning that prompts you to click **OK** or **Cancel**. If you click **OK** to continue, the oldest support bundle, which is listed in the warning message, is deleted. You can also delete support bundles using the CLI command `support bundle delete`.

Also, if you generate a support bundle on a upgraded system that contains a support bundle named using the old format, `support-bundle.tar.gz`, that file is renamed to use the newer name format.

4. Email the file to customer support at support@emc.com.

Note

If the bundle is too large to be emailed, use the EMC support site to upload the bundle. (Go to <https://support.emc.com>.)

Viewing the support bundles list

Use the Support Bundles tab to view the support bundle files on the system.

Procedure

1. Select a managed system in the Navigation panel.
2. Select **Maintenance** › **Support** › **Support Bundles**.

The Support Bundles list appears.

Listed are the support bundle file name, file size, and date the bundle was generated. Bundles are automatically named *hostname-support-bundle-datestamp.tar.gz*. An example filename is `localhost-support-bundle-1127103633.tar.gz`, which indicates that the support bundle was created on the localhost system on November 27th at 10:36:33.

3. Click the file name link and select a `gz/tar` decompression tool to view the ASCII contents of the bundle.

Alert notification management

The alert feature generates event and summary reports that can be distributed to configurable email lists and to EMC Data Domain.

Event reports are sent immediately and provide detailed information on a system event. The distribution lists for event alerts are called *notification groups*. You can configure a notification group to include one or more email addresses, and you can configure the types and severity level of the event reports sent to those addresses. For example, you might configure one notification group for individuals who need to know about critical events and another group for those who monitor less critical events. Another option is to configure groups for different technologies. For example, you might configure one notification group to receive emails about all network events and another group to receive messages about storage issues.

Summary reports are sent daily and provide a summary of the events that occurred during the last 24 hours. Summary reports do not include all the information provided in event reports. The default generation time for the daily report is 08.00 a.m, and it can be changed. Summary reports are sent using a dedicated email list that is separate from the event notification groups.

You can enable or disable alert distribution to EMC Data Domain. When sending reports to EMC, you have the option to select the legacy unsecure method or the ConnectEMC method, which encrypts the information before transmission.

Viewing the notification group list

A notification group is a configured group of email addresses (for subscribers) that defines the alert severity levels that are sent to the subscribers.

Procedure

1. Select **Status** › **Alerts** › **Notification**.
2. To limit (filter) the entries in the Group Name list, type a group name in the Group Name box or a subscriber email in the Alert Email box, and click **Update**.

Note

Click **Reset** to display all configured groups.

- To display detailed information for a group, select the group in the Group Name list.

Notification tab

The Notification tab allows you to configure groups of email address that receive system alerts for the alert types and severity levels you select.

Table 42 Group Name list, column label descriptions

Item	Description
Group Name	The configured name for the group.
Classes	The number of alert classes that are reported to the group.
Subscribers	The number of subscribers who are configured to receive notifications through email.

Table 43 Detailed Information, label descriptions

Item	Description
Class	A service or subsystem that can forward alerts. The listed classes are those for which the notification group receives alerts.
Severity	The severity level that triggers an email to the notification group. All alerts at the specified severity level and above are sent to the notification group.
Subscribers	The subscribers area displays a list of all email addresses configured for the notification group.

Table 44 Notification tab controls

Control	Description
Add button	Click the Add button to begin creating a notification group.
Class Attributes Configure button	Click this Configure button to change the classes and severity levels that generate alerts for the selected notification group.
Delete button	Click the Delete button to delete the selected notification group.
Filter By: Alert Email box	Enter text in this box to limit the group name list entries to groups that include an email address that contains the specified text.
Filter By: Group Name box	Enter text in this box to limit the group name list entries to group names that contain the specified text.

Table 44 Notification tab controls (continued)

Control	Description
Modify button	Click the Modify button to modify the configuration for the selected notification group.
Reset button	Click this button to remove any entries in the Filter By boxes and display all group names.
Subscribers Configure button	Click this Configure button to change the email list for the selected notification group.
Update button	Click this button to update the group name list after you enter text in a filter box.

Creating a notification group

Use the Notification tab to add notification groups and select the severity level for each group.

Procedure

1. Expand **DD Network** in the Navigation panel and select a managed system.
2. Select **Status > Alerts > Notification**.
3. Click **Add**.
The Add Group dialog box appears.
4. Type the group name in the **Group Name** box.
5. Select the checkbox of one or more alert classes of which to be notified.
6. To change the default severity level (Warning) for a class, select another level in the associated list box.
7. Click **OK**.

Managing the subscriber list for a group

Use the Notification tab to add, modify, or delete email addresses from a notification group subscriber list.

Procedure

1. Expand **DD Network** in the Navigation panel and select a managed system.
2. Select **Status > Alerts > Notification**.
3. Select the checkbox of a group in the Notifications group list, and do one of the following.
 - Click **Modify** and select **Subscribers**.
 - Click **Configure** in the Subscribers list.
4. To add a subscriber to the group, do the following.
 - a. Click the **+** icon.
The Email Address dialog box appears.

- b. Enter the email address of a subscriber.
 - c. Click **OK**.
5. To modify an email address, do the following.
 - a. Click the checkbox of the email address in the **Subscriber Email** list.
 - b. Click the pencil icon.
 - c. Edit the email address in the Email Address dialog box.
 - d. Click **OK**.
6. To delete an email address, click the checkbox of the email address in the **Subscriber Email** list and click the **X** icon.
7. Click **Finish** or **OK**.

Modifying a notification group

Use the Notification table to modify the attribute classes in an existing group.

Procedure

1. Expand DD Network in the Navigation panel and select a system.
2. Select **Status > Alerts > Notification**.
3. Select the checkbox of the group to modify in the group list.
4. To modify the class attributes for a group, do the following.
 - a. Click **Configure** in the Class Attributes area.
The Edit Group dialog box appears.
 - b. Select (or clear) the checkbox of one or more class attributes.
 - c. To change the severity level for a class attribute, select a level from the corresponding list box.
 - d. Click **OK**.
5. To modify the subscriber list for a group, do the following.
 - a. Click **Configure** in the Subscribers area.
The Edit Subscribers dialog box appears.
 - b. To delete subscribers from the group list, select the checkboxes of subscribers to delete and click the Delete icon (**X**).
 - c. To add a subscriber, click the Add icon (+), type a subscriber email address, and click **OK**.
 - d. Click **OK**.
6. Click **OK**.

Deleting a notification group

Use the Notification tab to delete one or more existing notification groups.

Procedure

1. Expand **DD Network** in the Navigation panel and select a managed system.
2. Select **Status > Alerts > Notification**.
3. Select one or more checkboxes of groups in the Notifications group list, and click **Delete**.

The Delete Group dialog box appears.

4. Verify the deletion and click **OK**.

Resetting the notification group configuration

Use the Notification tab to remove all notification groups added and to remove any changes made to the Default group.

Procedure

1. Expand **DD Network** in the Navigation panel and select a managed system.
2. Select **Status > Alerts > Notification**.
3. Select **More Tasks > Reset Notification Groups**.
4. In the Reset Notification Groups dialog box, click **Yes** in the verification dialog.

Configuring the daily summary schedule and distribution list

Every morning, each managed system sends a Daily Alert Summary email to the subscribers configured for the alertsummary.list email group. The Daily Alert Summary email contains current and historical alerts showing messages about non-critical hardware situations and disk space usage numbers that you might want to address soon.

A fan failure is an example of a noncritical issue that you might want to address as soon as is reasonably possible. When Support receives the failure notification, they contact you to arrange for component replacement.

Procedure

1. Expand **DD Network** in the Navigation panel and select a managed system.
2. Select **Status > Alerts > Daily Alert Summary**.
3. If the default deliver time of 8 AM is not acceptable, do the following.
 - a. Click **Schedule**.
The Schedule Alert Summary dialog box appears.
 - b. Use the list boxes to select the hour, minute, and either AM or PM for the summary report.
 - c. Click **OK**.
4. To configure the daily alert subscriber list, do the following.
 - a. Click **Configure**.
The Daily Alert Summary Mailing List dialog box appears.
 - b. Modify the daily alert subscriber list as follows.
 - To add a subscriber, click the **+** icon, type the email address, and click **OK**.
 - To modify an email address, select the checkbox for the subscriber, click the pencil icon, edit the email address, and click **OK**.
 - To delete an email address, select the checkbox for the subscriber and click **X**.
 - c. Click **Finish**.

Daily Alert Summary tab

The Daily Alert Summary tab allows you to configure an email list of those who want to receive a summary of all system alerts once each day. The people on this list do not receive individual alerts unless they are also added to a notification group.

Table 45 Daily Alert Summary, label descriptions

Item	Description
Delivery Time	The delivery time shows the configured time for daily emails.
Email List	This list displays the email addresses of those who receive the daily emails.

Table 46 Daily Alert Summary tab controls

Control	Description
Configure button	Click the Configure button to edit the subscriber email list.
Schedule button	Click the Schedule button to configure the time that the daily report is sent.

Enabling and disabling alert notification to EMC

By default, alert reports are enabled and sent daily to EMC Data Domain Customer Support using the legacy email method. The ConnectEMC method sends messages in a secure format using email, FTP, or HTTPS. You can use either method, or you can disable alert reporting to EMC.

Procedure

- To view the autosupport reporting status, select **Maintenance** > **Support** > **Autosupport**.
The autosupport notification status is highlighted in green in the Alert Support area.
- To display the selected EMC notification method, enter the CLI command: `support notification method show`.
- To enable alert reporting using the legacy method, do the following.
 - If ConnectEMC notification is selected, enter the command: `support notification method set email`.
 - In DD SM, select **Maintenance** > **Support** > **Autosupport**.
 - Select **Enable** in the Alert Support area.
- To enable alert reporting using ConnectEMC, do the following.
 - Verify that an administrator email is configured on the system by entering the `config show admin-email` command.
A system administrator email must be configured before you can select the ConnectEMC method.
 - To configure a system administrator email address, enter the `config set admin-email email-addr` command.

- c. If legacy email notification is selected, enter the command: `support notification method set connectemc`.
 - d. In DD SM, select **Maintenance** › **Support** › **Autosupport**.
 - e. Select **Enable** in the Alert Support area.
5. To disable alert reporting to EMC, do the following.
- a. In DD SM, select **Maintenance** › **Support** › **Autosupport**.
 - b. Select **Disable** in the Alert Support area.

Testing the alerts email feature

Use the Notification tab to send a test email to select notification groups or email addresses. This feature allows you to determine if the system is configured correctly to send alert messages.

Procedure

1. To control whether or not a test alert is sent to EMC Data Domain, do the following.
 - a. Select **Maintenance** › **Support** › **Autosupport**.
 - b. In the **Alert Support** area, click **Enable** or **Disable** to control whether or not the test email is sent .
You cannot change the email address.
2. Select **Status** › **Alerts** › **Notification**.
3. Select **Send Test Alert** from the More Tasks menu.
The Send Test Alert dialog box appears.
4. In the **Notification Groups** list, select groups to receive the test email and click **Next**.
5. Optionally, add additional email addresses to receive the email.
6. Click **Send Now** and **OK**.
7. If you disabled sending of the test alert to EMC Data Domain and you want to enable this feature now, do the following.
 - a. Select **Maintenance** › **Support** › **Autosupport**.
 - b. In the **Alert Support** area, click **Enable** .

Results

To test newly added alerts emails for mailer problems, enter: `autosupport test email email-addr`

For example, after adding the email address `djones@yourcompany.com` to the list, check the address with the command: `autosupport test email djones@yourcompany.com`

ConnectEMC management

ConnectEMC management controls allow you to view the configuration, status, and history of ConnectEMC communications, make configuration changes, and test ConnectEMC notification.

The initial configuration of ConnectEMC is included in the procedures for enabling reporting to EMC for alerts and autosupport reports.

The default transport method and protocol for ConnectEMC is direct email, but you can also configure primary and alternate transports that forward messages through an EMC

Secure Remote Support (ESRS) gateway. One advantage of the ESRS gateway is that one gateway can forward messages from multiple systems, and this allows you to configure network security for only the ESRS gateway instead of for multiple systems.

Viewing the ConnectEMC configuration, status, and history

Use the CLI to display the ConnectEMC configuration and the current ConnectEMC operational status. You can also display a report that lists each file sent to EMC with the transport protocol, time, and status of that transmission.

Procedure

1. To display the ConnectEMC configuration, enter the command: `support connectemc show config`
2. To display the ConnectEMC status, enter the command: `support connectemc status`
3. To display the ConnectEMC report history, enter the command: `support connectemc show history`

Setting and resetting the primary transport

The primary transport is the preferred transport method for autosupport and alert messages sent through ConnectEMC. The default primary transport is direct email.

You can configure only one primary transport. The direct method sends messages by secure email or FTPS directly to EMC. The ESRS-gateway method sends messages to an EMC Secure Remote Support (ESRS) gateway at the specified IP address (or resolvable hostname) using the specified protocol.

Procedure

1. To set the primary transport, enter the command: `support connectemc config set {direct [transport {email}] | esrs-gateway ip-address [transport {email | ftp | https}]}`

If you omit the transport protocol, the default protocol for the direct method is email, and the default protocol for the ESRS-gateway method is HTTPS.

2. To reset the primary transport to direct email, enter the command: `support connectemc config reset`

Adding and deleting alternate transports

An alternate transport sends autosupport and alert messages for ConnectEMC when the primary transport is not available. You can configure multiple alternates.

The direct method sends messages by secure email directly to EMC. The ESRS-gateway method sends messages to an EMC Secure Remote Support (ESRS) gateway at the specified IP address (or resolvable hostname) using the specified protocol.

Procedure

1. To add an alternate transport, enter the command: `support connectemc config add alternate {direct [transport {email}] | esrs-gateway ip-address [transport {email | ftp | https}]}`

If you omit the transport protocol, the default protocol for the ESRS-gateway method is HTTPS.

2. To delete an alternate transport, enter the command: `support connectemc config del alternate {direct [transport {email}] | esrs-gateway ip-address [transport {email | ftp | https}]}`

Configuring administrator notification

ConnectEMC can send email notification to the system administrator when autosupport or alert messages are sent to EMC. The administrator notification option allows you to disable administrator notification, notify the administrator whenever updates are sent to EMC, or notify the administrator only when transport failures occur. The default setting alerts the administrator only when an error occurs.

Procedure

1. To configure administrator notification, specify `onfailure` or `always` in the command: `support connectemc config set notify-admin {none | onfailure | always}`
2. To disable administrator notification, enter the command: `support connectemc config set notify-admin none`

Testing ConnectEMC operation

A CLI command allows you to test ConnectEMC operation by sending a dummy file to the system administrator.

Before you begin

A system administrator address must be configured for the system, and you must disable ConnectEMC reporting before the test.

Procedure

1. To disable ConnectEMC, enter `support notification method set email`.
2. To test ConnectEMC operation, enter `support connectemc test`.

```
#support connectemc test
Connection Record working successfully
```

After you finish

When the test is complete, enable ConnectEMC with `support notification method set connectemc`.

Log file management

The Data Domain system maintains a set of log files, which can be bundled and sent to EMC Support to assist in troubleshooting any system issues that may arise. Log files cannot be modified or deleted by any user with DD System Manager, but you can copy them from the log directory and manage them off of the system.

Log files are rotated weekly. Every Sunday at 0:45 a.m., the system automatically opens new log files for the existing logs and renames the previous files with appended numbers. For example, after the first week of operation, the previous week `messages` file is renamed `messages . 1`, and new messages are stored in a new `messages` file. Each numbered file is rolled to the next number each week. For example, after the second week, the file `messages . 1` is rolled to `messages . 2`. If a `messages . 2` file already existed, it rolls to `messages . 3`. At the end of the retention period (shown in the table below, the expired log is deleted. For example, an existing `messages . 9` file is deleted when `messages . 8` rolls to `messages . 9`.

Except as noted in this topic, the log files are stored in `/ddvar/log`.

Note

Files in the `/ddvar` directory can be deleted using Linux commands if the Linux user is assigned *write* permission for that directory.

The set of log files on each system is determined by the features configured on the system and the events that occur. The following table describes the log files that the system can generate.

Table 47 System log files

Log File	Description	Retention Period
audit.log	Messages about user log-in events.	15 weeks
cifs.log	Log messages from the CIFS subsystem are logged only in <code>debug/cifs/cifs.log</code> . Size limit of 50 MiB.	10 weeks
messages	Messages about general system events, including commands executed.	9 weeks
secure.log	Messages regarding user events such as successful and failed logins, user additions and deletions, and password changes. Only Admin role users can view this file.	9 weeks
space.log	<p>Messages about disk space usage by system components, and messages from the clean process. A space use message is generated every hour. Each time the clean process runs, it creates approximately 100 messages. All messages are in comma-separated-value format with tags you can use to separate the disk space messages from the clean process messages. You can use third-party software to analyze either set of messages. The log file uses the following tags.</p> <ul style="list-style-type: none"> • CLEAN for data lines from clean operations. • CLEAN_HEADER for lines that contain headers for the clean operations data lines. • SPACE for disk space data lines. • SPACE_HEADER for lines that contain headers for the disk space data lines. 	A single file is kept permanently. There is no log file rotation for this log.

Viewing log files in DD System Manager

Use the Logs tab to view and open the system log files in DD System Manager.

Procedure

1. In the Navigation panel, expand **DD Network** and select a managed system.
2. Select **Maintenance** > **Logs**.

The Logs list displays log file names and the size and generation date for each log file.

3. Click a log file name to view its contents. You may be prompted to select an application, such as Notepad.exe, to open the file.

Displaying a log file in the CLI

Use the `log view` command to view a log file in the CLI.

Procedure

1. To view a log file in the CLI, use the `log view` command.

With no argument, the command displays the current messages file.

2. When viewing the log, use the up and down arrows to scroll through the file; use the `q` key to quit; and enter a slash character (`/`) and a pattern to search through the file.

The display of the messages file is similar to the following. The last message in the example is an hourly system status message that the Data Domain system generates automatically. The message reports system uptime, the amount of data stored, NFS operations, and the amount of disk space used for data storage (%). The hourly messages go to the system log and to the serial console if one is attached.

```
# log view
Jun 27 12:11:33 localhost rpc.mountd: authenticated unmount
request from perfsun-g.emc.com:668 for /ddr/coll/segfs (/ddr/
coll/segfs)

Jun 27 12:28:54 localhost sshd(pam_unix)[998]: session opened
for user jsmith10 by (uid=0)

Jun 27 13:00:00 localhost logger: at 1:00pm up 3 days, 3:42,
52324 NFS ops, 84763 GiB data col. (1%)
```

Note

GiB = Gibibytes = the binary equivalent of Gigabytes.

Learning more about log messages

Look up error messages in the Error Message Catalog for your DD OS version.

In the log file is text similar to the following.

```
Jan 31 10:28:11 syrah19 bootbin: NOTICE: MSG-SMTOOL-00006: No
replication throttle schedules found: setting throttle to
unlimited.
```

The components of the message are as follows.

```
DateTime Host Process [PID]: Severity: MSG-Module-MessageID: Message
```

Severity levels, in descending order, are: Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug.

Procedure

1. Go to the EMC Online Support website at <https://support.emc.com>, enter *Error Message Catalog* in the search box, and click the search button.
2. In the results list, locate the catalog for your system and click on the link.

3. User your browser search tool to search for a unique text string in the message.

The error message description looks similar to the following display.

```
ID: MSG-SMTOOL-00006 - Severity: NOTICE - Audience: customer

Message: No replication throttle schedules found: setting
throttle to unlimited.

Description: The restorer cannot find a replication
throttle schedule. Replication is running with throttle set
to unlimited.

Action: To set a replication throttle schedule, run the
replication throttle add command.
```

4. To resolve an issue, do the recommended action.

Based on the example message description, one could run the `replication throttle add` command to set the throttle.

Saving a copy of log files

Save log file copies to another device when you want to archive those files.

Use NFS, CIFS mount, or FTP to copy the files to another machine. If using CIFS or NFS, mount `/ddvar` to your desktop and copy the files from the mount point. The following procedure describes how to use FTP to move files to another machine.

Procedure

1. On the Data Domain system, use the `adminaccess show ftp` command to see whether FTP service is enabled. If the service is disabled, use the command `adminaccess enable ftp`.
2. On the Data Domain system, use the `adminaccess show ftp` command to see that the FTP access list includes the IP address of your remote machine. If the address is not in the list, use the command `adminaccess add ftp ipaddr`.
3. On the remote machine, open a web browser.
4. In the **Address** box at the top of the web browser, use FTP to access the Data Domain system as shown in the following example.

```
ftp://Data Domain system_name.yourcompany.com/
```

Note

Some web browsers do not automatically ask for a login if a machine does not accept anonymous logins. In that case, add a user name and password to the FTP line. For example:

```
ftp://sysadmin:your-pw@Data Domain
system_name.yourcompany.com/
```

5. At the login pop-up, log into the Data Domain system as user `sysadmin`.
6. On the Data Domain system, you are in the directory just above the log directory. Open the log directory to list the messages files.
7. Copy the file that you want to save. Right-click the file icon and select **Copy To Folder** from the menu. Choose a location for the file copy.

8. If you want the FTP service disabled on the Data Domain system, after completing the file copy, use SSH to log into the Data Domain system as `sysadmin` and invoke the command `adminaccess disable ftp`.

Log message transmission to remote systems

Some log messages can be sent from the Data Domain system to other systems. DD OS uses `syslog` to publish log messages to remote systems.

A Data Domain system exports the following `facility.priority` selectors for log files. For information on managing the selectors and receiving messages on a third-party system, see your vendor-supplied documentation for the receiving system.

- `*.notice`—Sends all messages at the notice priority and higher.
- `*.alert`—Sends all messages at the alert priority and higher (alerts are included in `*.notice`).
- `kern.*`—Sends all kernel messages (kern.info log files).
- `local7.*`—Sends all messages from system startups (boot.log files).

The `log host` commands manage the process of sending log messages to another system.

Viewing the log file transmission configuration

Use the `log host show` CLI command to view whether log file transmission is enabled and which hosts receive log files.

Procedure

1. To display the configuration, enter the `log host show` command.

```
# log host show
Remote logging is enabled.
Remote logging hosts
    log-server
```

Enabling and disabling log message transmission

You must use CLI commands to enable or disable log message transmission.

Procedure

1. To enable sending log messages to other systems, use the `log host enable` command.
2. To disable sending log messages to other systems, use the `log host disable` command.

Adding or removing a receiver host

You must use CLI commands to add or remove a receiver host.

Procedure

1. To add a system to the list that receives Data Domain system log messages, use the `log host add` command.
2. To remove a system from the list that receives system log messages, use the command: `log host del`.

The following command adds the system named *log-server* to the hosts that receive log messages.

```
log host add log-server
```

The following command removes the system named *log-server* from the hosts that receive log messages.

```
log host del log-server
```

Remote system power management with IPMI

Select DD systems support remote power management using the Intelligent Platform Management Interface (IPMI), and they support remote monitoring of the boot sequence using Serial over LAN (SOL).

IPMI runs independently of DD OS and allows an IPMI user to manage system power as long as the remote system is connected to a power source and a network. An IP network connection is required between a management host and a remote system. When properly configured and connected, IPMI management eliminates the need to be physically present to power on or power off a remote system.

SOL is used to view the boot sequence after a power cycle on a remote system. SOL enables text console data that is normally sent to a serial port or to a directly attached console to be sent over a LAN and displayed by a management host.

You can use DD System Manager to configure IPMI for any managed system that appears in the Navigation panel. After you configure IPMI for a managed system, you can quickly begin remote system power management by selecting the managed system and entering the IPMI user information. Power management is easier for managed systems because you control the remote system configuration and do not need to remember the host name or IP address.

Note

If a system cannot support IPMI due to hardware or software limitations, DD System Manager displays a notification message when attempting to navigate to a configuration page.

The DD OS CLI allows you to configure a remote system for IPMI and SOL, and the CLI allows you to view the remote console output.

NOTICE

IPMI power removal is provided for emergency situations during which attempts to shut down power using DD OS commands fail. IPMI power removal simply removes power to the system, it does not perform an orderly shutdown of the DD OS file system. The proper way to remove and reapply power is to use the DD OS `system reboot` command. The proper way to remove system power is to use the DD OS `system poweroff` command and wait for the command to properly shut down the file system.

IPMI and SOL limitations

IPMI and SOL support is limited on some Data Domain systems.

- IPMI is supported on all systems supported by this release except the following systems: DD140, DD610, and DD630.
- IPMI user support varies as follows.
 - Model DD990: Maximum user IDs = 15. Three default users (NULL, anonymous, root). Maximum user IDs available = 12.
 - Models DD640, DD4200, DD4500, DD7200, and DD9500: Maximum user IDs = 10. Two default users (NULL, root). Maximum user IDs available = 8.
 - Model 690: Maximum user IDs = 10. One default user (root). Maximum user IDs available = 9.
- SOL is supported on the following systems: DD160, DD620, DD640, DD670, DD860, DD880, DD890, DD990, DD2200, DD2500 (requires DD OS 5.4.0.6 or later), DD4200, DD4500, DD7200, and DD9500.

Note

User root is not supported for IPMI connections on DD160 and DD880 systems.

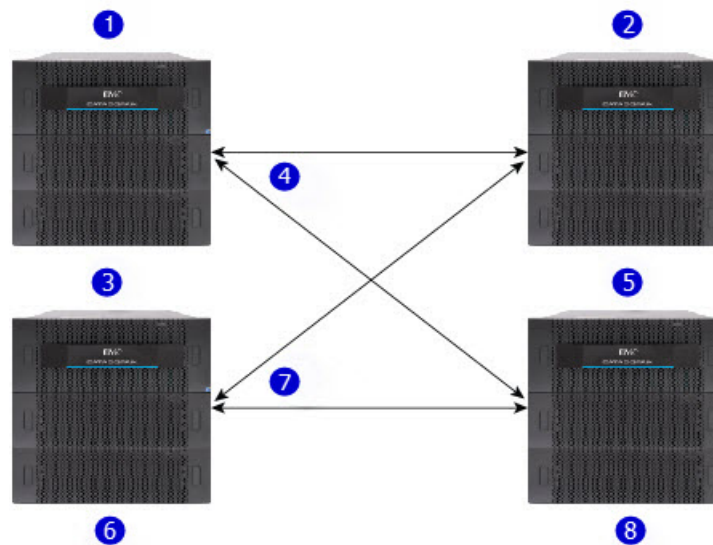
IPMI and SOL terminology

When multiple systems participate in IPMI and SOL, special names are used to describe the status and role of each system.

- **Management host**—The management host is the system you use to manage power on a remote system. When you use DD System Manager, the management host is the system you select in the Navigation panel. When you use the Data Domain OS CLI, the management host is the system on which you are using the CLI. Some specifications refer to the management system as the initiator.
- **Remote system**—A remote system is the target system for which you want to manage power. DD System Manager supports management of remote systems that are and are not managed by DD System Manager.
- **Managed remote system**—A managed remote system is a system that appears in the DD System Manager Navigation panel. You can use DD System Manager to configure IPMI on a managed system, and then you can use DD System Manager to manage power on that system.
- **Nonmanaged remote system**—A nonmanaged remote system is a system that does not appear in the DD System Manager Navigation panel. You can use DD System Manager to manage power on a nonmanaged system, but the nonmanaged system must be configured to support IPMI users before you can manage it. If a remote system is managed by another DD System Manager host, you can use the current DD System Manager host to manage it, but you manage it as a nonmanaged remote system because it is not configured in the current DD System Manager host.

Note

You can use the Data Domain OS CLI to enable IPMI and configure IPMI users on a nonmanaged remote host.

Figure 3 IPMI and SOL components and connections

1. Management hosts
2. Remote systems
3. DD System Manager
4. IPMI
5. Managed
6. CLI management
7. IPMI/SOL
8. Non-managed

Adding and deleting IPMI users with DD System Manager

Each managed system contains its own list of configured IPMI users. To enable a user to manage power on a managed system, you must add the user and configure a user password on the managed system.

To give an IPMI user the authority to manage power on multiple managed systems, you must add that user to each of the managed systems.

Note

The IPMI user list for each managed system is separate from the DD System Manager lists for administrator access and local users. Administrators and local users do not inherit any authorization for IPMI power management.

Procedure

1. Expand **DD Network** in the Navigation panel and select a managed system.
2. Select **Maintenance > IPMI**.
3. To add a user, complete the following steps.
 - a. Above the IPMI Users table, click **Add**.
 - b. In the Add User dialog box, type the user name (16 or less characters) and password in the appropriate boxes (reenter the password in the **Verify Password** box).

- c. Click **Create**.

The user entry appears in the **IPMI Users** table.

4. To delete a user, complete the following steps.
 - a. In the IPMI Users list, select a user and click **Delete**.
 - b. In the Delete User dialog box, click **OK** to verify user deletion.

Changing an IPMI user password

Use the IPMI tab to change the password for a user.

Procedure

1. Expand DD Network in the Navigation panel and select a managed system.
2. Select **Maintenance** › **IPMI**.
3. In the IPMI Users table, select a user, and click **Change Password**.
4. In the Change Password dialog box, type the password in the appropriate text box and reenter the password in the **Verify Password** box.
5. Click **Update**.

Configuring an IPMI port on a managed system

When you configure a port for a managed system, you select the port from a network ports list and specify the IP configuration parameters for that port. The selection of ports displayed depends on the Data Domain system selected.

Some systems support one or more dedicated ports, which can be used only for IPMI traffic. Other systems support ports that can be used for both IPMI traffic and all IP traffic supported by the physical interfaces in the **Hardware** › **Network** › **Interfaces** view. Shared ports are not provided on systems that provide dedicated IPMI ports.

The port names in the IPMI Network Ports list use the prefix `bmc`, which represents baseboard management controller. To determine if a port is a dedicated port or shared port, compare the rest of the port name with the ports in the network interface list. If the rest of the IPMI port name matches an interface in the network interface list, the port is a shared port. If the rest of the IPMI port name is different from the names in the network interface list, the port is a dedicated IPMI port.

Note

DD4200, DD4500, and DD7200 systems are an exception to the naming rule described earlier. On these systems, IPMI port, `bmc0a`, corresponds to shared port `ethMa` in the network interface list. EMC recommends that the shared port `ethMa` be reserved for IPMI traffic and system management traffic (using protocols such as HTTP, Telnet, and SSH). Backup data traffic should be directed to other ports.

When IPMI and nonIPMI IP traffic share an Ethernet port, EMC recommends that you do not use the link aggregation feature on the shared interface because link state changes can interfere with IPMI connectivity.

Procedure

1. Select the managed system in the Navigation panel.
2. Select **Maintenance** › **IPMI**.

The IPMI Configuration area shows the IPMI configuration for the managed system. The Network Ports table lists the ports on which IPMI can be enabled and configured. The IPMI Users table lists the IPMI users who can access the managed system.

Table 48 Network Ports list column descriptions

Item	Description
Port	The logical name for a port that supports IPMI communications.
Enabled	Whether the port is enabled for IPMI (Yes or No).
DHCP	Whether the port uses DHCP to set its IP address (Yes or No).
MAC Address	The hardware MAC address for the port.
IP Address	The port IP address.
Netmask	The subnet mask for the port.
Gateway	The gateway IP address for the port.

Table 49 IPMI Users list column descriptions

Item	Description
User Name	The name of a user with authority to power manage the remote system.

- In the **Network Ports** table, select a port to configure.

Note

If the IPMI port also supports IP traffic (for administrator access or backup traffic), the interface port must be enabled before you configure IPMI.

- Above the **Network Ports** table, click **Configure**.

The Configure Port dialog box appears.

- Choose how network address information is assigned.
 - To collect the IP address, netmask, and gateway configuration from a DHCP server, select **Dynamic (DHCP)**.
 - To manually define the network configuration, select **Static (Manual)** and enter the IP address, netmask, and gateway address.
- Enable a disabled IPMI network port by selecting the network port in the **Network Ports** table, and clicking **Enable**.
- Disable a disabled IPMI network port by selecting the network port in the **Network Ports** table, and clicking **Disable**.
- Click **Apply**.

Preparing for remote power management and console monitoring with the CLI

Remote console monitoring uses the Serial Over Lan (SOL) feature to enable viewing of text-based console output without a serial server. You must use the CLI to set up a system for remote console monitoring.

Remote console monitoring is typically used in combination with the `ipmi remote power cycle` command to view the remote system's boot sequence. This procedure should be used on every system for which you might want to remotely view the console during the boot sequence.

Procedure

1. Connect the console to the system directly or remotely.
 - Use the following connectors for a direct connection.
 - DIN-type connectors for a PS/2 keyboard (except DD880)
 - USB-A receptacle port for a USB keyboard
 - DB15 female connector for a VGA monitor

Note

Systems DD4200, DD4500, and DD7200 do not support direct connection, including KVM.

- For a serial connection, use a standard DB9 male or micro-DB9 female connector. Systems DD4200, DD4500, and DD7200 provide a female micro-DB9 connector. A null modem cable with male micro-DB9 and standard female DB9 connectors is included for a typical laptop connection.
 - For a remote IPMI/SOL connection, use the appropriate RJ45 receptacle as follows.
 - For DD880 systems, use either of the built-in Ethernet ports.
 - For DD990 systems, use default port `eth0d`.
 - For other systems, use the maintenance or service port. For port locations, refer to the system documentation, such as a hardware overview or installation and setup guide.
2. To support remote console monitoring, adjust the BIOS settings according to the model.
 - For models DD640, DD4200, DD4500, DD 7200 and DD990, use the default settings and proceed to step 3.
 - For model DD690, press F2 to go to BIOS. Click **Advanced** > **Serial Port Configuration** > **Serial B Enable [Enabled]**. Next, click **Server Management** > **Console Redirection** > **Serial Port B** > **Baud Rate 9.6K** and proceed to step 3.
 3. To display the IPMI port name, enter `ipmi show config`.
 4. To enable IPMI, enter `ipmi enable {port | all}`.
 5. To configure the IPMI port, enter `ipmi config port { dhcp | ipaddress ipaddr netmask mask gateway ipaddr }`.

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.

6. If this is the first time using IPMI, run `ipmi user reset` to clear IPMI users that may be out of synch between two ports, and to disable default users.
7. To add a new IPMI user, enter `ipmi user add user`.
8. To set up SOL, do the following:
 - a. Enter `system option set console lan`.
 - b. When prompted, enter `y` to reboot the system.

Managing power with DD System Manager

After IPMI is properly set up on a remote system, you can use DD System Manager to log into the remote system, view the power status, and change the power status.

Procedure

1. Log in to the remote system.
 - a. Expand **DD Network** in the Navigation panel and select a managed system that is different from the remote system you want to manage.

When you select a system in the Navigation panel, it becomes the management system and you cannot use IPMI to manage the management system. You can use a management system to manage remote systems only.
 - b. Select **Maintenance > IPMI**.
 - c. In the IPMI Power Management area, click **Login to Remote System**.
The IPMI Power Management dialog box appears.
 - d. In the Target System area, select the type of remote system and identify the system:
 - **Managed System**—Select a system in the **Managed** list box.
 - **Nonmanaged System**—Enter the IP address or hostname of the remote system in the **Another System** box.

SSH access to remote systems is not supported. If no system appears in the Managed list box, you must configure a managed system for IPMI before you continue. Nonmanaged systems must also be configured to support power management before you begin power management.
 - e. Enter the IPMI user name and password for the remote system.
 - f. Click **Connect**.
2. View the IPMI status.

The IPMI Power Management dialog box appears and shows the target system identification and the current power status. The Status area always shows the current status.

Note

The Refresh icon (the blue arrows) next to the status can be used to refresh the configuration status (for example, if the IPMI IP address or user configuration were changed within the last 15 minutes using the CLI commands).

3. To change the IPMI power status, click the appropriate button.
 - **Power Up**—Appears when the remote system is powered off. Click this button to power up the remote system.
 - **Power Down**—Appears when the remote system is powered on. Click this button to power down the remote system.
 - **Power Cycle**—Appears when the remote system is powered on. Click this button to power cycle the remote system.
 - **Manage Another System**—Click this button to log into another remote system for IPMI power management.
 - **Done**—Click to close the IPMI Power Management dialog box.

NOTICE

The IPMI Power Down feature does not perform an orderly shutdown of the DD OS. This option can be used if the DD OS hangs and cannot be used to gracefully shutdown a system.

Managing power with the CLI

You can manage power on a remote system and start remote console monitoring using the CLI.

Note

The remote system must be properly set up before you can manage power or monitor the system.

Procedure

1. Establish a CLI session on the system from which you want to monitor a remote system.
 2. To manage power on the remote system, enter `ipmi remote power {on | off | cycle | status} ipmi-target <ipaddr | hostname> user user.`
 3. To begin remote console monitoring, enter `ipmi remote console ipmi-target <ipaddr | hostname> user user.`
-

Note

The user name is an IPMI user name defined for IPMI on the remote system. DD OS user names are not automatically supported by IPMI.

4. To disconnect from a remote console monitoring session and return to the command line, enter the at symbol (@).
5. To terminate remote console monitoring, enter the tilde symbol (~).

CHAPTER 4

Monitoring Data Domain Systems

This chapter includes:

- [Viewing the summary status for all managed systems](#)..... 136
- [Viewing individual system status and identity information](#)..... 137
- [Alerts tab](#)..... 140
- [Viewing and clearing current alerts](#)..... 140
- [Viewing the alerts history](#)..... 141
- [Viewing hardware component status](#)..... 143
- [Viewing system statistics](#)..... 145
- [Viewing active users](#)..... 147
- [History report management](#)..... 147
- [Viewing the Task Log](#)..... 154

Viewing the summary status for all managed systems

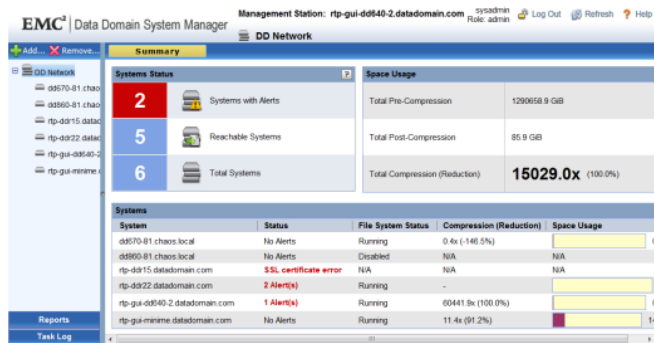
The DD Network Summary presents key statistics about the health of all managed Data Domain systems. The System Status, Space Usage, and Systems panels provide information to help you recognize problems immediately and determine which system is experiencing a problem.

Procedure

1. Select the DD Network icon in the Navigation panel.

The DD Network Summary view appears. It presents a high-level view of important information for the systems in the network. The summary view displays summary statistics for all managed systems, space usage statistics, and status for individual systems.

Figure 4 DD Network status display



System Status area

The Systems Status area displays a summary of the systems managed by the system you are logged into.

Table 50 Systems Status statistics

Item	Description
Systems with Alerts	The number of systems with active alerts.
Reachable Systems	The total number of systems reporting to the DD System Manager. A system may not be reporting if: <ul style="list-style-type: none"> • the system is offline • the network path to the system is down • an SSL certificate error occurred
Total Systems	The total number of managed systems configured on this DD System Manager system.

Space Usage area

The Space Usage list displays combined statistics for all managed systems.

Table 51 Space Usage statistics

Item	Description
Total Pre-Compression	The total amount of data sent to all managed systems by backup servers. This is the data written before compression.
Total Post-Compression	The total data amount for all systems after compression is performed.
Average Compression (Reduction)	The average amount of compression as calculated for each individual system.

Systems area

The Systems list summarizes important data for each of the managed systems.

Table 52 Systems list, column label descriptions

Item	Description
System	The name of a managed system.
Status	If the system is reachable, No Alerts or <i>n</i> Alerts appears, where <i>n</i> is the number of active alerts. The status line changes to red with an active alert. If the system is not reachable, the status column displays one of the following: <ul style="list-style-type: none"> Unknown Not reachable SSL certificate error
File System Status	The status of the file system. Status can be: <ul style="list-style-type: none"> Running Disabled N/A—The system is not reachable.
Compression (Reduction)	The average amount of compression for the listed system or N/A if the system is not reachable.
Space Usage	A bar graph showing the disk space in use or N/A if the system is not reachable.

Viewing individual system status and identity information

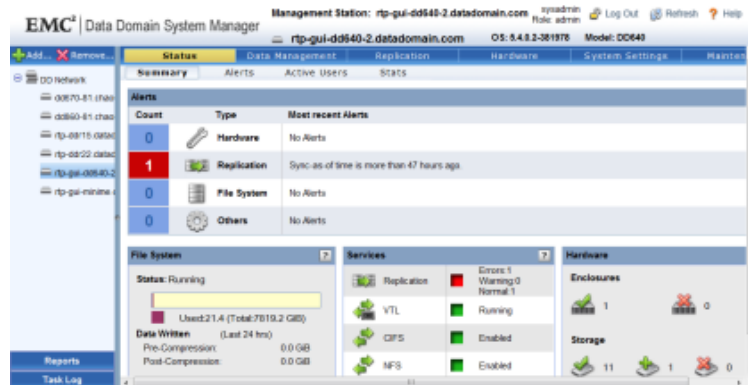
Two separate areas present individual system status and system identity information. The Status Summary area displays summary information and status for alerts, the file system, licensed services, and hardware enclosures. The Maintenance System area

displays the system uptime, system and chassis serial numbers, system model number, and DD OS version and build numbers.

Procedure

1. Select the system you want to view in the Navigation panel.
2. To view summary status information (which does not include the system uptime), select **Status > Summary**.

Figure 5 System summary status



3. To view the system uptime and identity information, select **Maintenance > System**.
The system uptime appears in the System area on the System tab.

Alerts area

The Alerts summary shows the count, type, and the text of the most recent alerts in the system for each subsystem (hardware, replication, file system, and others). Click anywhere in the alerts area to display more information on the current alerts.

Table 53 Alerts area column descriptions

Column	Description
Count	A count of the current alerts for the subsystem type specified in the adjacent column. The background color indicates the severity of the alert.
Type	The subsystem that generated the alert.
Most recent alerts	The text of the most recent alert for the subsystem type specified in the adjacent column

File System area

The File System summary displays statistics for the entire file system. Click anywhere in the File System area to display more information on the file system.

Table 54 File System area label descriptions

Column	Description
Status	The current status of the file system.
X.Xx	The average compression reduction factor for the file system.

Table 54 File System area label descriptions (continued)

Column	Description
Used	The total file system space being used.
Data Written: Pre-compression	The data quantity received by the system prior to compression.
Data Written: Post-compression	The data quantity stored on the system after compression.

Services area

The Services summary displays the status of the replication, VTL, CIFS, NFS, and DD Boost services. Click on a service to display detailed information about that service.

Table 55 Services area column descriptions

Column	Description
Left column	The left column lists the services that may be used on the system. These service can include replication, VTL, CIFS, NFS, and DD Boost.
Right column	The right column shows the operational status of the service. For most services, the status is enabled, disabled, or not licensed. The replication service row displays the number of replication contexts that are in normal, warning, and error states. A color coded box displays green for normal operation, yellow for warning situations, or red when errors are present).

Hardware area

The Hardware summary displays the status of the system enclosures and drives. Click anywhere in the hardware area to display more information on these components.

Table 56 Hardware area label descriptions

Label	Description
Enclosures	The enclosure icons display the number of enclosures operating in the normal (green checkmark) and degraded (red X) states.
Storage	The storage icons display the number of disk drives operating in the normal (green checkmark), spare (green +), or failed (red X) state.

System area

The System area on the System tab displays the system model number, DD OS version, system uptime, and system and chassis serial numbers.

Table 57 System area label descriptions

Label	Description
Model Number	The model number is the number assigned to the EMC Data Domain system.

Table 57 System area label descriptions (continued)

Label	Description
Version	The version is the DD OS version and build number of the software running on the system.
System Uptime	The system uptime displays how long the system has been running since the last system start. The time in parenthesis indicates when the system uptime was last updated.
System Serial No.	The system serial number is the serial number assigned to the system. On newer systems, such as DD4500 and DD7200, the system serial number is independent of the chassis serial number and remains the same during many types of maintenance events, including chassis replacements. On legacy systems, such as DD990 and earlier, the system serial number is set to the chassis serial number.
Chassis Serial No.	The chassis serial number is the serial number on the current system chassis.

Alerts tab

Alerts are messages from system services and subsystems that report system events. The Status > Alerts tab displays additional tabs that allow you to view current and non-current alerts, the configured alert notification groups, and the configuration for those who want to receive daily alert summary reports.

Alerts are also sent as SNMP traps. See the *MIB Quick Reference Guide* or the SNMP MIB for the full list of traps.

Viewing and clearing current alerts

The current alerts tab displays a list of all the current alerts and can display detailed information for a selected alert. An alert is automatically removed from the Current Alerts list when the underlying situation is corrected or when manually cleared.

Procedure

- To view all of the current alerts, select **Status > Alerts > Current Alerts**.
- To limit the number of entries in the current alert list, do the following.
 - In the Filter By area, select a **Severity** and **Class** to expose only alerts that pertain to those choices.
 - Click **Update**.
All alerts not matching the Severity and Class are removed from the list.
- To display additional information for a specific alert in the **Details** area, click the alert in the list.
- To clear an alert, select the alert checkbox in the list and click **Clear**.
A cleared alert no longer appears in the current alerts list, but it can be found in the alerts history list.
- To remove filtering and return to the full listing of current alerts, click **Reset**.

Current Alerts tab

The Current Alerts tab displays a list of alerts and detailed information about a selected alert.

Table 58 Alerts list, column label descriptions

Item	Description
ID	A unique numerical identifier for the alert.
Message	The alert message text.
Severity	The level of seriousness of the alert. For example, warning, critical, info, or emergency.
Date	The time and date the alert occurred.
Class	The subsystem where the alert occurred.
Object	The physical component where the alert is occurring.
Status (Alerts History tab only)	Whether the status is posted or cleared. A posted alert is not cleared.

Table 59 Details area, row label descriptions

Item	Description
Alert ID	A unique numerical identifier for the alert.
Name	A textual identifier for the alert.
Message	The alert message text.
Severity	The level of seriousness of the alert. For example, warning, critical, info, emergency.
Class	The subsystem and device where the alert occurred.
Date	The time and date the alert occurred.
Object ID	The physical component where the alert is occurring.
Event ID	An event identifier.
Tenant Units	Lists affected tenant units.
Description	More descriptive information about the alert.
Action	A suggestion to remedy the alert.
SNMP OID	SNMP object ID.

Viewing the alerts history

The Alerts History tab displays a list of all the cleared alerts and can display detailed information for a selected alert.

Procedure

1. To view all of the alerts history, select **Status > Alerts > Alerts History**.

2. To limit the number of entries in the current alert list, do the following.
 - a. In the Filter By area, select a **Severity** and **Class** to expose only alerts that pertain to those choices.
 - b. Click **Update**.
All alerts not matching the Severity and Class are removed from the list.
3. To display additional information for a specific alert in the **Details** area, click the alert in the list.
4. To remove filtering and return to the full listing of cleared alerts, click **Reset**.

Alerts History tab

The Alerts History tab displays a list of cleared alerts and details about a selected alert.

Table 60 Alerts list, column label descriptions

Item	Description
ID	A unique numerical identifier for the alert.
Message	The alert message text.
Severity	The level of seriousness of the alert. For example, warning, critical, info, or emergency.
Date	The time and date the alert occurred.
Class	The subsystem where the alert occurred.
Object	The physical component where the alert is occurring.
Status	The current disposition of the alert (for example, Posted or Cleared).

Table 61 Details area, row label descriptions

Item	Description
Alert ID	A unique numerical identifier for the alert.
Name	A textual identifier for the alert.
Message	The alert message text.
Severity	The level of seriousness of the alert. For example, warning, critical, info, emergency,
Class	The subsystem and device where the alert occurred.
Date	The time and date the alert occurred.
Object ID	The physical component where the alert is occurring.
Event ID	An event identifier.
Tenant Units	Lists affected tenant units.
Additional Information	More descriptive information about the alert.
Type	The type of alert.
Status	The status of the alert.

Table 61 Details area, row label descriptions (continued)

Item	Description
Clear By	The user name that cleared the alert.

Viewing hardware component status

The Chassis tab displays a block drawing of each enclosure in a system, including the chassis serial number and the enclosure status. Within each block drawing are the enclosure components, such as disks, fans, power supplies, NVRAM, CPUs, and memory. The components that appear depend upon the system model.

On systems running DD OS 5.5.1 and later, the system serial number is also displayed. On newer systems, such as DD4500 and DD7200, the system serial number is independent of the chassis serial number and remains the same during many types of maintenance events, including chassis replacements. On legacy systems, such as DD990 and earlier, the system serial number is set to the chassis serial number.

Procedure

1. Expand DD Network in the Navigation panel and select a system.
2. Select **Hardware > Chassis**.

The Chassis view shows the system enclosures. Enclosure 1 is the system controller, and the rest of the enclosures appear below Enclosure 1.

Components with problems show yellow (warning) or red (error); otherwise, the component displays OK.

3. Hover the cursor over a component to see detailed status.

Fan status

Fans are numbered and correspond to their location in the chassis. Hover over a system fan to display a tooltip for that device.

Table 62 Fan tooltip, column label descriptions

Item	Description
Description	The name of the fan.
Level	The current operating speed range (Low, Medium, High). The operating speed changes depending on the temperature inside the chassis.
Status	The health of the fan.

Temperature status

Data Domain systems and some components are configured to operate within a specific temperature range, which is defined by a temperature profile that is not configurable. Hover over the Temperature box to display the temperature tooltip.

Table 63 Temperature tooltip, column label descriptions

Item	Description
Description	<p>The location within the chassis being measured. The components listed depend on the model and are often shown as abbreviations. Some examples are:</p> <ul style="list-style-type: none"> • CPU 0 Temp (Central Processing Unit) • MLB Temp 1 (main logic board) • BP middle temp (backplane) • LP temp (low profile of I/O riser FRU) • FHFL temp (full height full length of I/O riser FRU) • FP temp (front panel)
C/F	<p>The C/F column displays temperature in degrees Celsius and Fahrenheit. When the description for a CPU specifies <i>relative</i> (CPU <i>n</i> Relative), this column displays the number of degrees that each CPU is below the maximum allowable temperature and the actual temperature for the interior of the chassis (chassis ambient).</p>
Status	<p>Shows the temperature status:</p> <ul style="list-style-type: none"> • OK—The temperature is acceptable • Critical—The temperature is higher than the shutdown temperature. • Warning—The temperature is higher than the warning temperature (but lower than the shutdown temperature). • Dash (-) —No temperature thresholds are configured for this component, so there is no status to report.

Power supply status

The tooltip shows the status of the power supply (OK or DEGRADED if a power supply is absent or failed). You can also look at the back panel of the enclosure and check the LED for each power supply to identify those that need replacing.

PCI slot status

The PCI slots shown in the chassis view indicate the number of PCI slots and the numbers of each slot. Tooltips provide component status for each card in a PCI slot. For example, the NVRAM tooltip displays the firmware version, memory size, temperature data, and battery levels.

NVRAM status

Hover over NVRAM to display information about the Non-Volatile RAM, batteries, and other components.

Table 64 NVRAM tooltip, column label descriptions

Item	Description
Component	<p>The items in the component list depend on the NVRAM installed in the system and can include the following items.</p> <ul style="list-style-type: none"> • Firmware version • Memory size • Error counts • Flash controller error counts • Board temperature • CPU temperature • Battery number (The number of batteries depends on the system type.) • Current slot number for NVRAM
C/F	<p>Displays the temperature for select components in the Celsius/Fahrenheit format.</p>
Value	<p>Values are provided for select components and describe the following.</p> <ul style="list-style-type: none"> • Firmware version number • Memory size value in the displayed units • Error counts for memory, PCI, and controller • Flash controller error counts sorted in the following groups: configuration errors (Cfg Err), panic conditions (Panic), Bus Hang, bad block warnings (Bad Blk Warn), backup errors (Bkup Err), and restore errors (Rstr Err) • Battery information, such percent charged and status (enabled or disabled)

Viewing system statistics

The Stats tab displays up to five graphs that show real-time subsystem performance statistics, such as CPU usage and disk traffic.

Procedure

1. Expand **DD Network** in the Navigation panel and select a system.
2. Select **Status > Stats**.

The Performance Graphs area displays the currently selected graphs.

3. To change the selection of graphs to display, select and clear the checkboxes for graphs in the list box.

4. To view specific data-point information, hover over a graph point.
5. When a graph contains multiple data, you can use the checkboxes in the upper-right corner of the graph to select what to display. For example, if Read is not selected in the upper right of the disk activity graph, only write data is graphed.

Results

Each graph shows usage over the last 200 seconds. Click **Pause** to temporarily stop the display. Click **Resume** to restart it and show points missed during the pause.

Performance statistics graphs

The performance statistics graphs display statistics for key system components and features.

DD Boost

The DD Boost graph displays the bytes/second transferred for each of the past 200 seconds. Separate lines within the graph display the rates for data read from the system by DD Boost clients and data written to the system by DD Boost clients.

Disk

The Disk graph displays the amount of data in the appropriate unit of measurement based on the data received, such as KiB or MiB per second, going to and from all disks in the managed system.

File System Operations

The File System Operations graph displays the number of operations per second that occurred for each of the past 200 seconds. Separate lines within the graph display the NFS and CIFS operations per second.

Network

The Network graph displays the amount of data in the appropriate unit of measurement based on the data received, such as KiB or MiB per second, that passes through each Ethernet connection. One line appears for each Ethernet port.

Recent CPU Usage

The Recent CPU Usage graph displays the percentage of CPU usage for each of the past 200 seconds.

Replication (DD Replicator must be licensed)

The Replication graph displays the amount of replication data traveling over the network for each of the last 200 seconds. Separate lines display the In and Out data as follows:

- In: The total number of units of measurement, such as kilobytes per second, received by this side from the other side of the Replicator pair. For the destination, the value includes backup data, replication overhead, and network overhead. For the source, the value includes replication overhead and network overhead.
- Out: The total number of units of measurement, such as kilobytes per second, sent by this side to the other side of the Replicator pair. For the source, the value includes backup data, replication overhead, and network overhead. For the destination, the value includes replication and network overhead.

Viewing active users

The Active Users tab displays the names of users who are logged into the system and statistics about the current user sessions.

Procedure

1. Expand **DD Network** in the Navigation panel and select a system.
2. Select **Status > Active Users**.

The Active Users list appears and displays information for each user.

Table 65 Active Users list, column label descriptions

Item	Description
Name	User name of the logged-in user.
Idle	Time since last activity of user.
Last Login From	System from which the user logged in.
Last Login Time	Datestamp of when user logged in.
TTY	Terminal notation for login. GUI appears for DD System Manager users.

Note

To manage local users, click **Go to Local Users**.

History report management

DD System Manager enables you to generate reports to track space usage on a Data Domain system for up to the previous two years. You can also generate reports to help understand replication progress, and view daily and cumulative reports on the file system.

The Reports view is divided into two sections. The upper section lets you create the various types of reports. The lower section lets you view and manage saved reports.

Reports display in a table format, and as charts, depending on the type of report. You can select a report for a specific Data Domain system and provide a specific time period.

The reports display historical data, not real-time data. After the report is generated, the charts remain static and do not update. Examples of the types of information you can get from the reports include:

- The amount of data that was backed up to the system and the amount of de-duplication that was achieved
- Estimates of when the Data Domain system will be full, based on weekly space usage trends
- Backup and compression utilization based on selected intervals
- Historical cleaning performance, including duration of cleaning cycle, amount of space that can be cleaned, and amount of space that was reclaimed

- Amount of WAN bandwidth used by replication, for source and destination, and if bandwidth is sufficient to meet replication requirements
- System performance and resource utilization

Types of reports

The New Report area lists the types of reports you can generate on your system.

Note

Replication reports can only be created if the system contains a replication license and a valid replication context is configured.

File System Cumulative Space Usage report

The File System Cumulative Space Usage Report displays 3 charts that detail space usage on the system during the specified duration. This report is used to analyze how much data is backed up, the amount of deduplication performed, and how much space is consumed.

Table 66 File System—Usage chart label descriptions

Item	Description
Data Written (GiB)	The amount of data written before compression. This is indicated by a purple shaded area on the report.
Time	The timeline for data that was written. The time displayed on this report changes based upon the Duration selection when the chart was created.
Total Compression Factor	The total compression factor reports the compression ratio.

Table 67 File System—Consumption chart label descriptions

Item	Description
Used (GiB)	The amount of space used after compression.
Time	The date the data was written. The time displayed on this report changes based upon the Duration selection when the chart was created.
Post Comp	The amount of storage used after compression.
Usage Trend	The dotted black line shows the storage usage trend. When the line reaches the red line at the top, the storage is almost full.
Size and Cleaning	Size is the Total Capacity on a Data Domain system. Cleaning is the Cleaning cycle (start and end time for each cleaning cycle). Administrators can use this information to choose the best time for space cleaning the best throttle setting.

Table 68 File System Weekly Cumulative Capacity chart label descriptions

Item	Description
Date (or Time for 24 hour report)	The last day of each week, based on the criteria set for the report. In reports, a 24-hour period ranges from noon-to-noon.
Data Written (Pre-Comp)	The cumulative data written before compression for the specified time period.
Used (Post-Comp)	The cumulative data written after compression for the specified time period.
Total Compression Factor	The total compression factor. This is indicated by a black line on the report.

File System Daily Space Usage report

The File System Daily Space Usage report displays five charts that detail space usage during the specified duration. This report is used to analyze daily activities.

Table 69 File System Daily Space Usage chart label descriptions

Item	Description
Space Used (GiB)	The amount of space used. Post-comp is red shaded area. Pre-Comp is purple shaded area.
Time	The date the data was written.
Compression Factor	The total compression factor. This is indicated by a black square on the report.

Table 70 File System Daily Capacity Utilization chart label descriptions

Item	Description
Date	The date the data was written.
Data Written (Pre-Comp)	The amount of data written pre-compression.
Used (Post-Comp)	The amount of storage used after compression.
Total Compression Factor	The total compression factor.

Table 71 File System Weekly Capacity Utilization chart label descriptions

Item	Description
Start Date	The first day of the week for this summary.
End Date	The last day of the week for this summary.
Available	Total amount of storage available.
Consumed	Total amount of storage used.
Data (Post -Comp)	The cumulative data written before compression for the specified time period.

Table 71 File System Weekly Capacity Utilization chart label descriptions (continued)

Item	Description
Replication (Post-Comp)	The cumulative data written after compression for the specified time period.
Overhead	Extra space used for non-data storage.
Reclaimed by Cleaning	The total space reclaimed after cleaning.

Table 72 File System Compression Summary chart label descriptions

Item	Description
Time	The period of data collection for this report.
Data Written (Pre-Comp)	The amount of data written pre-compression.
Used (Post-Comp)	The amount of storage used after compression.
Total Compression Factor	The total compression factor.

Table 73 File System Cleaning Activity chart label descriptions

Item	Description
Start Time	The time the cleaning activity started.
End Time	The time the cleaning activity finished.
Duration (Hours)	The total time required for cleaning in hours.
Space Reclaimed	The space reclaimed in Gibibytes (GiB).

Replication Status report

The Replication Status report displays three charts that provide the status of the current replication job running on the system. This report is used to provide a snapshot of what is happening for all replication contexts to help understand the overall replication status on a Data Domain System.

Table 74 Replication Context Summary chart label descriptions

Item	Description
ID	The Replication Context identification.
Source	Source system name.
Destination	Destination system name.
Type	Type of replication context: MTree, Directory, Collection, or Pool.
Status	Replication status types include: Error, Normal.
Sync as of Time	Time and date stamp of last sync.
Estimated Completion	The estimated time the replication should be complete.

Table 74 Replication Context Summary chart label descriptions (continued)

Item	Description
Pre-Comp Remaining	The amount of pre-compressed data to be replicated. This only applies to Collection type.
Post-Comp Remaining	The amount of post-compressed data to be replicated. This only applies to Directory and Pool types.

Table 75 Replication Context Error Status chart label descriptions

Item	Description
ID	The Replication Context identification.
Source	Source system name.
Destination	Destination system name.
Type	Replication context type: Directory or Pool.
Status	Replication status types include: Error, Normal, and Warning.
Description	Description of the error.

Table 76 Replication Destination Space Availability chart label descriptions

Item	Description
Destination	Destination system name.
Space Availability (GiB)	Total amount of storage available.

Replication Summary report

The Replication Summary report provides performance information about a system's overall network in-and-out usage for replication, as well as per context levels over a specified duration. You select the contexts to be analyzed from a list.

Table 77 Replication Summary report label descriptions

Item	Description
Network In (MiB)	The amount of data entering the system. Network In is indicated by a thin green line.
Network Out (MiB)	The amount of data sent from the system. Network Out is indicated by a thick orange line.
Time	The date on which the data was written.
Pre-Comp Remaining (MiB)	The amount of pre-compressed data to be replicated. Pre-Comp Remaining is indicated by a blue line.

Creating a report

To create a new report, select the report options in the the New Report area and click **Create**.

Procedure

1. In the Navigation panel, click the **Reports** button.
The information panel displays a new report area and a list of saved reports.
2. Click a report type in the New Report area.
3. In the System menu, select the system for which you want to create a report .
4. Select additional options for the report based on the type of report.
 - Duration— Last 4 Weeks, Last 7 Days, or Custom
 - Contexts—Available contexts for working with the Replication Summary report

Note

In reports, the duration of a 24-hour day ranges from noon-to-noon.

5. If you select Custom for the duration, enter Start and End Date and Time in the additional fields.
6. Click **Create**.

The report appears in a separate browser window and is added to the end of the Saved Reports list.

Note

If the report does not display, verify the option to block pop-up windows is enabled on your browser.

Viewing saved reports

After you create a report, you can view it using the controls in the Save Reports area.

Procedure

1. In the Navigation panel, click the **Reports** button.
The information panel displays a new report area and a list of saved reports.
2. Select the report you want to view in the Saved Reports area.
3. Click **View**.
The report appears in a new browser window.

Note

If the report does not appear, verify the option to block pop-up windows is enabled on your browser.

Printing saved reports

After you create a report, you can print it using the controls in your browser window.

Procedure

1. In the Navigation panel, click **Reports**.
The Information panel displays a new report area and a list of saved reports.
2. Select the report you want to view in the Saved Reports area.
3. Click **View**.
The report appears in a new browser window.
4. In the browser window, select **File > Print**.

Deleting saved reports

You can delete any of the reports that appear in the Saved Reports area.

Procedure

1. In the Navigation panel, click the **Reports**.
The Information panel displays a new report area and a list of saved reports.
2. Select the report you want to delete in the Saved Reports area. You can select multiple reports to delete. Click the box at the top to select all reports.
3. Click **Delete**.
A warning dialog box asks if you are sure you want to delete the selected reports.
4. Click **OK**, and click **Close**.

Renaming saved reports

DD System Manager automatically names each report as it is created. You can rename any of the reports that appear in the Saved Reports area.

Procedure

1. In the Navigation panel, click **Reports**.
The information panel displays a new report area and a list of saved reports.
2. Select the report you want to rename in the **Saved Reports** area.
3. Click **Rename**.
The Rename Report dialog box appears.
4. Type a name for your report in the New Report Name box.
It is a good idea to give the report a simple, descriptive name you can easily recognize.
5. Click **OK**.

Viewing the Task Log

The Task Log displays a list of currently running jobs, such as, replication or system upgrades. DD System Manager can manage multiple systems and can initiate tasks on those systems. If a task is initiated on a remote system, the progress of that task is tracked in the management station task log, not in the remote system task log.

Procedure

1. In the Navigation panel, click **Task Log**.
The Tasks view appears.
2. Select a filter by which to display the Task Log from the Filter By list box. You can select **All**, **In Progress**, **Failed**, or **Completed**.
The Tasks view displays the status of all tasks based on the filter you select and refreshes every 60 seconds.
3. To manually refresh the Tasks list, do either of the following.
 - Click **Update** to update the task log.
 - Click **Reset** to display all tasks and remove any filters that were set.
4. To display detailed information about a task, select the task in the task list.

Table 78 Detailed Information, label descriptions

Item	Description
System	The descriptive name of the managed system.
Task Description	A description of the type of task.
Start Time	The date and time the task started.
Status	The status of the task (completed, failed, or in progress).
End Time	The date and time the task ended.
Error Message	An applicable error message, if any.

5. To return to the managing system, select the system in the Navigation panel.

CHAPTER 5

File System

This chapter includes:

- [File system overview](#)..... 156
- [Monitoring file system usage](#).....162
- [Managing file system operations](#)..... 168
- [Fast copy operations](#)..... 176

File system overview

Learn how to use the file system.

How the file system stores data

Data Domain storage capacity is best managed by keeping multiple backups and 20% empty space to accommodate backups until the next cleaning. Space use is primarily affected by the size and compressibility of data, and the retention period.

A Data Domain system is designed as a very reliable online system for backups and archive data. As new backups are added to the system, old backups are aged out. Such removals are normally done under the control of backup or archive software based on the configured retention period.

When backup software expires or deletes an old backup from a Data Domain system, the space on the Data Domain system becomes available only after the Data Domain system cleans the data of the expired backups from disk. A good way to manage space on a Data Domain system is to retain as many online backups as possible with some empty space (about 20% of total space available) to comfortably accommodate backups until the next scheduled cleaning, which runs once a week by default.

Some storage capacity is used by Data Domain systems for internal indexes and other metadata. The amount of storage used over time for metadata depends on the type of data stored and the sizes of the stored files. With two otherwise identical systems, one system may, over time, reserve more space for metadata and have less space for actual backup data than the other if different data sets are sent to each system.

Space utilization on a Data Domain system is primarily affected by:

- The size and compressibility of the backup data.
- The retention period specified in the backup software.

High levels of compression result when backing up datasets with many duplicates and retaining them for long periods of time.

How the file system reports space usage

All DD System Manager windows and system commands display storage capacity using base 2 calculations. For example, a command that displays 1 GiB of disk space as used reports 2^{30} bytes = 1,073,741,824 bytes.

- 1 KiB = 2^{10} = 1024 bytes
- 1 MiB = 2^{20} = 1,048,576 bytes
- 1 GiB = 2^{30} = 1,073,741,824 bytes
- 1 TiB = 2^{40} = 1,099,511,627,776 bytes

How the file system uses compression

The file system uses compression to optimize available disk space when storing data, so disk space is calculated two ways: physical and logical. (See the section regarding types of compression.) Physical space is the actual disk space used on the Data Domain system. Logical space is the amount of uncompressed data written to the system.

The file system space reporting tools (DD System Manager graphs and `filesys show space` command, or the alias `df`) show both physical and logical space. These tools also report the size and amounts of used and available space.

When a Data Domain system is mounted, the usual tools for displaying a file system's physical use of space can be used.

The Data Domain system generates warning messages as the file system approaches its maximum capacity. The following information about data compression gives guidelines for disk use over time.

The amount of disk space used over time by a Data Domain system depends on:

- The size of the initial full backup.
- The number of additional backups (incremental and full) retained over time.
- The rate of growth of the backup dataset.
- The change rate of data.

For data sets with typical rates of change and growth, data compression generally matches the following guidelines:

- For the first full backup to a Data Domain system, the compression factor is generally 3:1.
- Each incremental backup to the initial full backup has a compression factor generally in the range of 6:1.
- The next full backup has a compression factor of about 60:1.

Over time, with a schedule of weekly full and daily incremental backups, the aggregate compression factor for all the data is about 20:1. The compression factor is lower for incremental-only data or for backups with less duplicate data. Compression is higher when all backups are full backups.

Types of compression

Data Domain compresses data at two levels: global and local. Global compression compares received data to data already stored on disks. Duplicate data does not need to be stored again, while data that is new is locally compressed before being written to disk.

Local Compression

A Data Domain system uses a local compression algorithm developed specifically to maximize throughput as data is written to disk. The default algorithm (lz) allows shorter backup windows for backup jobs but uses more space. Local compression options provide a trade-off between slower performance and space usage. To change compression, see the section regarding changing local compression.

After you change the compression, all new writes use the new compression type. Existing data is converted to the new compression type during cleaning. It takes several rounds of cleaning to recompress all of the data that existed before the compression change.

The initial cleaning after the compression change might take longer than usual. Whenever you change the compression type, carefully monitor the system for a week or two to verify that it is working properly.

How the file system implements data integrity

Multiple layers of data verification are performed by the DD OS file system on data received from backup applications to ensure that data is written correctly to the Data Domain system disks. This ensures the data can be retrieved without error.

The DD OS is purpose-built for data protection and it is architecturally designed for data invulnerability. There are four critical areas of focus, described in the following sections.

End-to-end verification

End-to-end checks protect all file system data and metadata. As data comes into the system, a strong checksum is computed. The data is deduplicated and stored in the file

system. After all data is flushed to disk, it is read back, and re-checksummed. The checksums are compared to verify that both the data and the file system metadata are stored correctly.

Fault avoidance and containment

Data Domain uses a log-structured file system that never overwrites or updates existing data. New data is always written in new containers and appended to existing old containers. The old containers and references remain in place and are safe even in the face of software bugs or hardware faults that may occur when storing new backups.

Continuous fault detection and healing

Continuous fault detection and healing protects against storage system faults. The system periodically rechecks the integrity of the RAID stripes, and uses the redundancy of the RAID system to heal any faults. During a read, data integrity is re-verified and any errors are healed on the fly.

File system recoverability

Data is written in a self-describing format. The file system can be re-created, if necessary, by scanning the log and rebuilding it from the metadata stored with the data.

How the file system reclaims storage space with file system cleaning

When your backup application (such as NetBackup or NetWorker) expires data, the data is marked by the Data Domain system for deletion. However, the data is not deleted immediately; it is removed during a cleaning operation.

- During the cleaning operation, the file system is available for all normal operations including backup (write) and restore (read).
- Although cleaning uses a significant amount of system resources, cleaning is self-throttling and gives up system resources in the presence of user traffic.
- Data Domain recommends running a cleaning operation after the first full backup to a Data Domain system. The initial local compression on a full backup is generally a factor of 1.5 to 2.5. An immediate cleaning operation gives additional compression by another factor of 1.15 to 1.2 and reclaims a corresponding amount of disk space.
- When the cleaning operation finishes, a message is sent to the system log giving the percentage of storage space that was reclaimed.

A default schedule runs the cleaning operation every Tuesday at 6 a.m. (tue 0600). You can change the schedule or you can run the operation manually (see the section regarding modifying a cleaning schedule).

Data Domain recommends running the cleaning operation once a week.

Any operation that disables the file system, or shuts down a Data Domain system during a cleaning operation (such as a system power-off or reboot) aborts the cleaning operation. The cleaning operation does not immediately restart when the system restarts. You can manually restart the cleaning operation or wait until the next scheduled cleaning operation.

With MTree replication, if a file is created and deleted while a snapshot is being replicated, then the next snapshot will not have any information about this file, and the system will not replicate any content associated with this file. Directory replication will replicate both the create and delete, even though they happen close to each other.

With the replication log that directory replication uses, operations like deletions, renaming, and so on, execute as a single stream. This can reduce the replication throughput. The use of snapshots by MTree replication avoids this problem.

Supported interfaces

Interfaces supported by the file system.

- NFS
- CIFS
- DD Boost
- VTL

Supported backup software

Guidance for setting up backup software and backup servers to use with a Data Domain systems is available at support.emc.com.

Data streams sent to a data domain system

For optimal performance, Data Domain recommends limits on simultaneous streams between Data Domain systems and your backup servers.

A data stream, in the context of the following table, refers to a large byte stream associated with sequential file access, such as a write stream to a backup file or a read stream from a restore image. A Replication source or destination stream refers to a directory replication operation or a DD Boost file replication stream associated with a file replication operation.

Table 79 Data streams sent to a data domain system

Model	RAM/ NVRAM	Backup write streams	Backup read streams	Repl ¹ source streams	Repl ¹ dest streams	Mixed
DD140, DD160, DD610	4 GB or 6 GB / 0.5 GB	16	4	15	20	w<= 16 ; r<= 4 ReplSrc<=15; ReplDest<=20; ReplDest+w<=16; w+r+ReplSrc <=16; Total<=20
DD620, DD630, DD640	8 GB / 0.5 GB or 1 GB	20	16	30	20	w<=20; r<=16; ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; Total<=30
DD660	16 GB / 1 GB	90	30	60	90	w<=90; r<=30; ReplSrc <=60; ReplDest <= 90; ReplDest + w <= 90; Total <= 90
DD640, DD670, DD690	16 GB or 20 GB / 1 GB	90	30	60	90	w<=90; r<=30; ReplSrc<=60; ReplDest<=90; ReplDest+w<=90; Total<=90
DD690	24 GB / 1GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD670, DD860	36 GB / 1 GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90

Table 79 Data streams sent to a data domain system (continued)

Model	RAM/ NVRAM	Backup write streams	Backup read streams	Repl ¹ source streams	Repl ¹ dest streams	Mixed
DD860	72 GB ² / 1 GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD880	64 GB / 2 GB	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest+w<=180; Total<=180
DD890	96 GB / 2 GB	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest+w<=180; Total<=180
DD990	128 or 256 GB ² / 4 GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest+w<=540; Total<=540
DD2200	8 GB	35	6	26	35	w<=35; r<=6; ReplSrc <= 26; ReplDest <= 20; ReplDest+w <= 35; Total <= 35
DD2200	16 GB	60	16	56	42	w<=60; r<=16; ReplSrc <= 56; ReplDest <= 42; ReplDest+w <= 60; Total <= 60
DD2500	32 or 64 GB / 2 GB	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest+w<=180; Total<=180
DD4200	128 GB ² / 4 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest+w<=270; Total<=270
DD4500	192 GB ² / 4 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest+w<=270; Total<=270
DD7200	128 or 256 GB ² / 4 GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest+w<=540; Total<=540
DD9500	256/512 GB	1080	300	540	1080	w<=1080; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest+w<=1080; Total<=1080

1: DirRepl, OptDup, MTreeRepl streams. 2: The Data Domain Extended Retention software option is available only for these devices with extended (maximum) memory.

File system limitations

File system limitations, including: limits on the number of files, the battery, and so on.

Limits on number of files in a data domain system

Consequences and considerations of storing more than 1 billion files.

Data Domain recommends storing no more than 1 billion files on a system. Storing a larger number of files can adversely affect the performance and the length of cleaning, and some processes, such as file system cleaning, may run much longer with a very large number of files. For example, the enumeration phase of cleaning may take from a few minutes to several hours depending upon the number of files in the system.

Note

The overall performance for the Data Domain system will fall to unacceptable levels if the system is required to support the maximum file amount and the workload from the client machines is not carefully controlled.

When the file system passes the billion file limit, several processes or operations might be adversely affected, for example:

- Cleaning may take a very long time to complete, perhaps several days.
- AutoSupport operations may take more time.
- Any process or command that needs to enumerate all the files.

If there are many small files, other considerations arise:

- The number of separate files that can be created per second, (even if the files are very small) may be more of a limitation than the number of MB/s that can be moved into a Data Domain system. When files are large, the file creation rate is not significant, but when files are small, the file creation rate dominates and may become a factor. The file creation rate is about 100 to 200 files per second depending upon the number of MTrees and CIFS connections. This rate should be taken into account during system sizing when a bulk ingest of a large number of files is needed by a customer environment.
- File access latencies are affected by the number of files in a directory. To the extent possible, we recommend directory sizes of less than 10,000. Larger directory sizes will experience slower responses to metadata operations such as listing the files in the directory and opening or creating a file.

Limits on the battery

For systems that use NVRAM, the operating system creates a low battery alert if the battery charge falls below 80% capacity, and the file system is disabled.

NOTICE

The Data Domain DD2200 system does not use NVRAM so firmware calculations decide whether the battery charge is sufficient to save the data and disable the file system if there is a loss of AC power.

Maximum number of supported inodes

An NFS or CIFS client request causes a Data Domain system to report a capacity of about two billion inodes (files and directories). A Data Domain system can exceed that number, but the reporting on the client may be incorrect.

Maximum path name length

The maximum length of a full path name (including the characters in `/data/coll/backup`) is 1023 bytes. The maximum length of a symbolic link is also 1023 bytes.

Monitoring file system usage

View real-time data storage statistics.

The File System view has tabs that show real-time data storage statistics, including current compression factors showing the space saved by using data deduplication, graphs of space usage amounts, consumption factors, and data written trends. There are also some options for managing file system cleaning, expansion, copying, and destruction.

Accessing the file system view

This section describes the file system functionality.

Procedure

1. Select a system in the Navigation panel.
2. Click the **Data Management** > **File System** tabs.

The File System view has a **File System** overview panel and six tabs which are described in detail in this section.

About the file system overview panel

Display the file system state and the clean status.

State

The State area contains an **Enable/Disable** button and the shows the working state of the file system:

- Enabled and running—and the latest consecutive length of time the file system has been enabled and running.
- Disabled and shutdown.
- Enabling and disabling—in the process of becoming enabled or disabled.
- Destroying—if the file system is being deleted.
- Error—if there is an error condition, such as a problem initializing the file system.

Clean Status

The **Clean Status** area contains a **Start/Stop Cleaning** button and shows the date the last cleaning operation occurred, or the current cleaning status if the cleaning operation is currently running. For example:

```
Cleaning finished at 2009/01/13 06:00:43
```

or, if the file system is disabled, shows:

```
Unavailable
```

About the file system summary view

Click the Summary tab to view file system statistics.

File system space usage

Display the amount of disk space available and used by the file system components, based on the last cleaning.

- The `/data:post-comp` line shows amounts for compressed data in the `/data` directory.
- The `/ddvar` line shows amounts for log and core files. (Remove old logs and core files to free space in this area.)

Note

You can also delete core files from the `/ddvar/var/core` or the `/ddvar/ext` directory if it exists.

For both of these, the following amounts are shown in real numbers and in the color-coded graph as described in *About the Space Usage View (File System)*.

- Size—The amount of total physical disk space available for data.
- Used—the actual physical space used for compressed data. Warning messages go to the system log and an email alert is generated when the use reaches 90%, 95%, and 100%. At 100%, the Data Domain system accepts no more data from backup servers. If the Used amount is always high, check the cleaning schedule to see how often the cleaning operation runs automatically. Then use the modifying a cleaning schedule procedure to run the operation more often. Also consider reducing the data retention period or splitting off a portion of the backup data to another Data Domain system.
- Available (GiB)—The total amount of space available for data storage. This figure 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.
- Cleanable (GiB)—The amount of space that could be reclaimed if a cleaning were run.

The second Space Usage panel shows the compression factors:

- Currently Used—The amounts currently in use by the file system.
- Written in Last 24 Hours—The compression activity over the last day.

For both of these areas, the following is shown:

- Pre-Compression (GiB)—Data written before compression.
- Post-Compression (GiB)—Storage used after compression.
- Global-Comp Factor—Pre-Compression / (Size after global compression).
- Local-Comp Factor—(Size after global compression) / Post-Compression.
- Total-Comp Factor—Pre-Comp / Post-Comp.
- Reduction %— $[(\text{Pre-Comp} - \text{Post-Comp}) / \text{Pre-Comp}] * 100$.

About the retention units view

Display the retention unit and its state, its status, and its size.

The Retention Units view on the File System page is shown only when the optional DD Extended Retention license is enabled. This view lists the retention unit and shows its state (new, sealed, or target), its status (disabled or ready), and its size. If the unit has been sealed, meaning no more data can be added, the date that it was sealed is given.

Select the diamond symbol to the right of a column heading to sort the order of the values in reverse.

About the configuration view

Display and change system options as well as the current cleaning schedule.

Table 80 Option settings and descriptions

Options settings	Description
Local Compression Type	The type of local compression in use. <ul style="list-style-type: none"> See the section regarding types of compression for an overview. See the section regarding changing local compression
Report Replica as Writable	How applications see a replica. <ul style="list-style-type: none"> See the section regarding changing read-only settings
Marker Type	Backup software markers (tape markers, tag headers, or other names are used) in data streams. See the section regarding tape marker settings
Staging Reserve	Manage disk staging. <ul style="list-style-type: none"> See the section regarding working with disk staging See the section regarding configuring disk staging

Table 81 Cleaning Schedule Settings

Cleaning schedule settings	Description
Time	The date time cleaning operations run. <ul style="list-style-type: none"> See the section regarding modifying a cleaning schedule
Throttle	The system resources allocation. <ul style="list-style-type: none"> See the section regarding throttling the cleaning operation

About the encryption view

Display encryption status, progress, algorithms, and so on.

Table 82 Encryption settings

Setting	Description
Encryption	
Status	Status can be one of the following: <ul style="list-style-type: none"> Not licensed—No other information provided. Not configured—Encryption is licensed but not configured. Enabled—Encryption is enabled and running.

Table 82 Encryption settings (continued)

Setting	Description
Encryption Progress	<ul style="list-style-type: none"> Disabled—Encryption is disabled. <p>View encryption status details for the active tier regarding the application of changes and re-encryption of data. Status can be one of the following:</p> <ul style="list-style-type: none"> None Pending Running Done <p>Click View Details to display the Encryption Status Details dialog that includes the following information for the Active Tier:</p> <ul style="list-style-type: none"> Type (Example: Apply Changes when encryption has already been initiated, or Re-encryption when encryption is a result of compromised data—perhaps a previously destroyed key.) Status (Example: Pending) Details: (Example: Requested on December xx/xx/xx and will take after the next system clean).
Encryption Algorithm	<p>The algorithm used to encrypt the data:</p> <ul style="list-style-type: none"> AES 256-bit (CBC) (default) AES 256-bit (GCM) (more secure but slower) AES 128-bit (CBC) (not as secure as 256-bit) AES 128-bit (GCM) (not as secure as 256-bit) <p>See Changing the Encryption Algorithm for details.</p>
Encryption Passphrase	When configured, shows as “*****.” To change the passphrase, see Managing the System Passphrase.
File System Lock	
Status	<p>The File System Lock status is either:</p> <ul style="list-style-type: none"> Unlocked—The feature is not enabled. Locked—The feature is enabled.
Key Management	
Key Manager	Either the internal Data Domain Embedded Key Manager or the optional RSA Data Protection Manager (DPM) Key Manager. Click Configure to switch between key managers (if both are configured), or to modify Key Manager options.
Server	The name of the RSA Key Manager Server.
Server Status	Online or offline, or the error messages returned by the RSA Key Manager Server.
Key Class	A specialized type of security class used by the optional RSA Data Protection Manager (DPM) Key Manager that groups cryptographic keys with similar characteristics. The Data Domain system retrieves a

Table 82 Encryption settings (continued)

Setting	Description
	key from the RSA server by key class. A key class to be set up to either return the current key, or to generate a new key each time.
	<p>Note</p> <p>The Data Domain system supports only key classes configured to return the current key.</p>
Port	The port number of the RSA server.
FIPS mode	Whether or not the imported host certificate is FIPS compliant. The default mode is enabled.
Encryption Keys	<p>Lists keys by ID numbers. Shows when a key was created, how long it is valid, its type (RSA DPM Key Manager or the Data Domain internal key), its state (see Working with the RSA DPM Key Manager, DPM Encryption Key States Supported by Data Domain), and the amount of the data encrypted with the key.</p> <p>The system displays the last updated time for key information above the right column.</p> <p>Selected keys in the list can be:</p> <ul style="list-style-type: none"> • Synchronized so the list shows new keys added to the RSA server (but are not usable until the file system is restarted). • Deleted. • Destroyed.

About the space usage view (file system)

Display a visual (but static) representation of data use for the file system at certain points in time.

Click the **Data Management > File System > Space Usage** tabs.

- Click a point on a graph line to display a box with data at that point.
- Click **Print** (at the bottom on the graph) to open the standard Print dialog box.
- Click **Show in new window** to display the graph in a new browser window.

The lines of the graph denote measurement for:

- **Pre-comp Written**—The total amount of data sent to the MTree by backup servers. Pre-compressed data on an MTree is what a backup server sees as the total uncompressed data held by an MTree-as-storage-unit, shown with the Space Used (left) vertical axis of the graph.
- **Post-comp Used**—The total amount of disk storage in use on the MTree, shown with the Space Used (left) vertical axis of the graph.
- **Comp Factor**—The amount of compression the Data Domain system has performed with the data it received (compression ratio), shown with the Compression Factor (right) vertical axis of the graph.

Checking Historical Space Usage

On the Space Usage graph, clicking an interval (that is, 7d, 30d, 60d, or 120d) on the Duration line above the graph allows you to change the number of days of data shown on the graph, from 7 to 120 days.

To see space usage for intervals over 120 days, issue the following command:

```
# fileSYS show compression [summary | daily | daily-detailed] {[last n
{hours | days | weeks | months}] | [start date [end date]]}
```

About the consumption view

Display space used over time, in relation to total system capacity.

- Click a point on a graph line to display a box with data at that point.
- Click **Print** (at the bottom on the graph) to open the standard Print dialog box.
- Click **Show in new window** to display the graph in a new browser window.

The lines of the graph denote measurement for:

- **Capacity**—The total amount of disk storage available for data on the Data Domain system. The amount is shown with the Space Used (left) vertical axis of the graph. Clicking the Capacity checkbox toggles this line on and off.
- **Post-comp**—The total amount of disk storage in use on the Data Domain system. Shown with the Space Used (left) vertical axis of the graph.
- **Comp Factor**—The amount of compression the Data Domain system has performed with the data it received (compression ratio). Shown with the Compression Factor (right) vertical axis of the graph.
- **Cleaning**—A grey diamond is displayed on the chart each time a file system cleaning operation was started.
- **Data Movement**—The amount of disk space moved to the archiving storage area (if the Archive license is enabled).

Checking Historical Consumption Usage

On the Consumption graph, clicking an interval (that is, 7d, 30d, 60d, 120d) on the Duration line above the graph allows you to change the number of days of data shown on the graph, from 7 to 120 days.

About the daily written view (file system)

Display the flow of data over the last 24 hours. The data amounts are shown over time for pre- and post-compression amounts.

The system also provides totals for global and local compression amounts, and pre-compression and post-compression amounts.

- Click a point on a graph line to display a box with data at that point.
- Click **Print** (at the bottom on the graph) to open the standard Print dialog box.
- Click **Show in new window** to display the graph in a new browser window.

The lines on the graph denote measurements for:

- **Pre-Comp Written**—The total amount of data written to the file system by backup servers. Pre-compressed data on the file system is what a backup server sees as the total uncompressed data held by the file system.
- **Post-Comp Written**—The total amount of data written to the file system after compression has been performed, as shown in GiBs.

- **Total Comp Factor**—The total amount of compression the Data Domain system has performed with the data it received (compression ratio), shown with the Total Compression Factor (right) vertical axis of the graph.

Checking Historical Written Data

On the Daily Written graph, clicking an interval (that is, 7d, 30d, 60d, or 120d) on the Duration line above the graph allows you to change the number of days of data shown on the graph, from 7 to 120 days.

Below the Daily Written graph, the following totals display for the current duration value:

- Pre-Comp Written
- Post-Comp Written
- Global-Comp Factor
- Local-Comp Factor
- Total-Comp Factor

When the file system is full or nearly full

Data Domain systems have three progressive levels of being full. As each level is reached, more operations are progressively disallowed. At each level, deleting data and then performing a file system cleaning operation makes disk space available.

Note

The process of deleting files and removing snapshots does not immediately reclaim disk space, the next cleaning operation reclaims the space.

- **Level 1**—At the first level of fullness, no more new data can be written to the file system. An informative out of space alert is generated.
Remedy—Delete unneeded datasets, reduce the retention period, delete snapshots, and perform a file system cleaning operation.
- **Level 2**—At the second level of fullness, files cannot be deleted. This is because deleting files also require free space but the system has so little free space available that it cannot even delete files.
Remedy—Expire snapshots and perform a file system cleaning operation.
- **Level 3**—At the third and final level of fullness, attempts to expire snapshots, delete files, or write new data fail.
Remedy—Perform a file system cleaning operation to free enough space to at least delete some files or expire some snapshots and then rerun cleaning.

Monitor the space usage with email alerts

Alerts are generated when the file system is at 90%, 95%, and 100% full. To send these alerts, add the user to the alert emailing list.

Note

To join the alert email list, see [Viewing and Clearing Alerts](#).

Managing file system operations

This section describes file system cleaning, sanitization, and performing basic operations.

Performing basic operations

Basic file system operations include enabling and disabling the file system, and in the rare occasion, destroying a file system.

Creating the file system

Create a file system from the Data Management > File System page using the More Tasks menu.

There are three reasons to create a file system:

- For a new Data Domain system.
- When a system is started after a clean installation.
- After a file system has been destroyed.

To create the file system:

Procedure

1. Verify that storage has been installed and configured (see the section on viewing system storage information for more information). If the system does not meet this prerequisite, a warning message is displayed. Install and configure the storage before attempting to create the file system.
2. Select a system in the Navigation panel.
3. Click the **Data Management > File System** tabs.
4. From the **More Tasks** menu, select **Create File System**.

The File System Create dialog box shows the approximate size of the file system. Check **Enable file system** after creation to start using this file system as soon as it is created. Click **Next**.

5. A summary displays the file system size and whether the file system is to be automatically enabled. Click **Back** if you want to change the enable the file system option. Clicking **Finish** starts the file system creation.
6. A progress bar measures the file system creation's progress. A check mark indicates that a step of the procedure has completed. When a check mark Completed is displayed, click **OK**.

Enabling or disabling the file system

The option to enable or disable the file system is dependent on the current state of the file system—if its enabled, you can disable it and vice versa.

- Enabling the file system allows Data Domain system operations to begin. This ability is available to administrative users only.
- Disabling the file system halts all Data Domain system operations, including cleaning. This ability is available to administrative users only.

CAUTION

Disabling the file system when a backup application is sending data to the system can cause the backup process to fail. Some backup software applications are able to recover by restarting where they left off when they are able to successfully resume copying files; others might fail, leaving the user with an incomplete backup.

Procedure

1. Select a system in the Navigation panel.
2. Click the **Data Management** > **File System** tabs.
3. In the Overview panel, click **Enable** or **Disable** in the State area.
4. Click **OK** and **Close**.

Expanding the file system

You might need to expand the size of a file system if the suggestions given in "When the File System Is Full or Nearly Full" do not clear enough space for normal operations.

A file system may not be expandable, however, for these reasons:

- The file system is not enabled.
- There are no unused disks or enclosures in the Active or Retention tiers.
- An expanded storage license is not installed.
- There are not enough capacity licenses installed.

To expand the file system:

Procedure

1. Select a system in the Navigation panel.
2. Click the **Data Management** > **File System** tabs.
3. From the **More Tasks** menu, select **Expand Capacity**.

The Expand File System Capacity window displays the current capacity of the file system (active or retention tier) as well as how much additional storage space is available for expansion.

- If enough capacity is available for expansion requirements, continue to step 7.
- If capacity needs to be added, continue with the next step.

Note

If you are configuring a DD2200 system, click the Add License link in the Expand File System Capacity window and enter the CONTROLLER-COD license to expand storage to 7.5 TB, and the EXPANDED-STORAGE license to expand storage to 13.18 TB, and click Expand.

Note

File system capacity can be expanded only if the physical disks are installed on the system and file system is enabled.

4. Click **Configure** to allocate existing storage to the file system.
The Configure Storage dialog box is displayed.
5. In the Available Storage area, click the checkboxes of the storage devices to use and click **Add to Tier**.
System storage must be moved from the Available Storage area to the Active Tier storage area before the file system can be created.
6. Click **OK** and **Close** in the progress dialog box.

- Click **Finish** to expand the file system into the available storage.

Destroying the file system

Destroying the file system should be done only under the direction of Customer Support. This action deletes all data in the Data Domain file system, including virtual tapes. Deleted data is not recoverable. This operation also removes Replication configuration settings.

This operation is used when it is necessary to clean out existing data, to create a new collection replication destination, or to replace a collection source, or for security reasons because the system is being removed from operation.

CAUTION

The optional Write zeros to disk operation writes zeros to all file system disks, effectively removing all traces of data. If the Data Domain system contains a large amount of data, this operation can take many hours, or a day, to complete.

Note

As this is a destructive procedure, this operation is available to administrative users only.

Procedure

- From the **More Tasks** menu, select **Destroy**.
- In the Destroy File System dialog box, enter the sysadmin password (it is the only accepted password).
- Optionally, click the checkbox for **Write zeros to disk** to completely remove data.
- Click **OK**.

Performing cleaning

This section describes how to start, stop, and modify cleaning schedules.

Starting cleaning manually

To immediately start a cleaning operation.

Procedure

- In the Overview panel, click **Start Cleaning** in the Clean Status area.
The **Start File System Clean** dialog box is displayed.
- In the Throttle Percentage text box, enter a system throttle amount. This is the percentage of CPU usage dedicated to cleaning. The default is 50 percent.
- Click **OK**.

The Start File System Clean dialog box allows you to monitor the cleaning operation progress.

- Click **Close** to exit the progress dialog box.

Stopping cleaning manually

To immediately stop a cleaning operation.

WARNING

Stopping the cleaning process cancels all cleaning progress for the cleaning run.

Procedure

1. In the Overview panel, click **Stop Cleaning** in the **Clean Status** area.
The Stop File System Clean dialog box displays.
2. Click **OK**.

Modifying a cleaning schedule

Use the Modify Schedule dialog of the GUI to modify a cleaning schedule.

Procedure

1. Click the **Data Management > File System > Configuration** tabs.
2. In the Clean Schedule area, click **Edit**.
The Modify Schedule dialog box displays.
3. Select the cleaning frequency, such as daily, bi-weekly, or monthly. Weekly is the default.
4. Enter the start day of the week, time, and throttle percentage.

Note

Modify the throttle percentage only if necessary. Cleaning leverages all resources when they are idle.

5. Click **OK**.

Throttling the cleaning operation

Throttle settings to change the amount of system resources used by the cleaning process.

Use the *Modifying a Cleaning Schedule* section to change the system resources used by the cleaning process.

Performing sanitization

To comply with government guidelines, system sanitization, also called data shredding, must be performed when classified or sensitive data is written to any system that is not approved to store such data.

When an incident occurs, the system administrator must take immediate action to thoroughly eradicate the data that was accidentally written. The goal is to effectively restore the storage device to a state as if the event never occurred. If the data leakage is with sensitive data, the entire storage will need to be sanitized using EMC Professional Services' Secure Data erasure practice.

The Data Domain sanitization command exists to enable the administrator to delete files at the logical level, whether a backup set or individual files. Deleting a file in most file systems consists of just flagging the file or deleting references to the data on disk, freeing up the physical space to be consumed at a later time. However, this simple action introduces the problem of leaving behind a residual representation of underlying data physically on disks. Deduplicated storage environments are not immune to this problem.

Shredding data in a system implies eliminating the residual representation of that data and thus the possibility that the file may be accessible after it has been shredded. Data Domain's sanitization approach ensures is compliant with the 2007 versions of Department of Defense (DoD) 5220.22 of the following specifications:

- *US Department of Defense 5220.22-M Clearing and Sanitization Matrix*
- *National Institute of Systems and Technology (NIST) Special Publication 800-88 Guidelines for Media Sanitization*

Sanitizing deduplicated data

Data Domain systems sanitize data in place, in its native deduplicated state.

Deduplication storage systems extract common data patterns from files sent to the system and store only unique copies of these patterns, referencing all the redundant instances. Because these data patterns or segments may potentially be shared among many files in the system, the sanitization process must first determine whether each of the segments of the contaminated file are shared with a clean file and then erase only those segments that are not shared, along with any contaminated metadata.

All storage tiers, caches, unused capacity, and free space are cleared so that every copy of every segment that belongs exclusively to the deleted files is eradicated. The system reclaims and overwrites all of the storage occupied by these segments to effectively restore the storage device to a state as if the contaminated files never existed in that system.

Sanitization level 1: data clearing or shredding

If the data you need to remove is unclassified, as defined in the "US Department of Defense 5220.22-M Clearing and Sanitization Matrix," Level 1 sanitization can be used to overwrite the affected storage once. This provides the basis for handling most data shredding and system sanitization cases.

The Data Domain system sanitization feature ensures that every copy of every segment that belongs only to erased files is overwritten using a single-pass zerotization mechanism. Clean data in the system being sanitized is online and available to users.

Procedure

1. Delete the contaminated files or backups through the backup software or corresponding client. In the case of backups, be sure to manage the backup software appropriately to ensure that related files on that image are reconciled, catalog records are managed as required, and so forth.
2. Run the `system sanitize start` command on the contaminated Data Domain system to cause all previously used space in it to be overwritten once (see the figure below).
3. Wait for the affected system to be sanitized. Sanitization can be monitored by using the `system sanitize watch` command.

If the affected Data Domain system has replication enabled, all the systems containing replicas need to be processed in a similar manner. Depending on how much data exists in the system and how it is distributed, the `system sanitize` command could take some time. However, during this time, all clean data in the system is available to users.

Sanitization level 2: full system sanitization

If the data you need to remove is classified, as defined in the "US Department of Defense 5220.22-M Clearing and Sanitization Matrix," Level 2 sanitization, or full system sanitization, is now required.

Data Domain recommends Blancco for multi-pass overwrites with any overwrite pattern and a certificate. This provides the basis for handling universal Department of Defense requirements where complete system sanitization is required. For more information, go to:

https://www.emc.com/auth/rcoll/servicekitdocument/cp_datadomaindataerase_psbasddde.pdf

Modifying basic settings

Change the type of compression used, marker types, Replica write status, and Staging Reserve percentage, as described in this section.

Changing local compression

Use the Local Compression Type area of the GUI to select a new compression type.

Note

Do not change the type of local compression unless it is necessary.

Procedure

1. Click the **Data Management** > **File System** > **Configuration** tabs.
2. In the Options area, click **Edit**.
The Modify Settings dialog box displays.
3. In the Local Compression Type area, click the drop-down list and select a new compression type.

Table 83 Compression type

Option	Description
none	Do not compress data.
lz	The default algorithm that gives the best throughput. Data Domain recommends the lz option.
gzfast	A zip-style compression that uses less space for compressed data, but more CPU cycles (twice as much as lz). Gzfast is the recommended alternative for sites that want more compression at the cost of lower performance.
gz	A zip-style compression that uses the least amount of space for data storage (10% to 20% less than lz on average; however, some datasets get much higher compression). This also uses the most CPU cycles (up to five times as much as lz). The gz compression type is commonly used for nearline storage applications in which performance requirements are low.

4. Click **OK** at the confirmation dialog box.
5. Click **Close** to exit the status dialog box.

Changing read-only settings

Change the replica to writable. Some backup applications must see the replica as writable to do a restore or vault operation from the replica.

Procedure

1. Click the **Data Management** > **File System** > **Configuration** tabs.
2. In the Options area, click **Edit**.
The Modify Settings dialog box is displayed.

3. In the Report Replica as Writable area, click the **Enable** checkbox.
4. Click **OK**.
5. Click **Close** to exit the status dialog box.

Working with disk staging

Disk staging enables a Data Domain system to serve as a staging device, where the system is viewed as a basic disk via a CIFS share or NFS mount point.

Disk staging can be used in conjunction with your backup software, such as Symantec's NetBackup (NBU) and EMC's NetWorker, it does not require a license, and is disabled by default.

Note

The VTL feature is not required or supported when the Data Domain system is used as a Disk Staging device.

The reason that some backup applications use disk staging devices is to enable tape drives to stream continuously. After the data is copied to tape, it is retained on disk for as long as space is available. Should a restore be needed from a recent backup, more than likely the data is still on disk and can be restored from it more conveniently than from tape. When the disk fills up, old backups can be deleted to make space. This delete-on-demand policy maximizes the use of the disk.

In normal operation, the Data Domain System does not reclaim space from deleted files until a cleaning operation is done. This is not compatible with backup software that operates in a staging mode, which expects space to be reclaimed when files are deleted. When you configure disk staging, you reserve a percentage of the total space—typically 20 to 30 percent—in order to allow the system to simulate the immediate freeing of space.

The amount of available space is reduced by the amount of the staging reserve. When the amount of data stored uses all of the available space, the system is full. However, whenever a file is deleted, the system estimates the amount of space that will be recovered by cleaning and borrows from the staging reserve to increase the available space by that amount. When a cleaning operation runs, the space is actually recovered and the reserve restored to its initial size. Since the amount of space made available by deleting files is only an estimate, the actual space reclaimed by cleaning may not match the estimate. The goal of disk staging is to configure enough reserve so that you do not run out before cleaning is scheduled to run.

Configuring disk staging

Enable disk staging and specify the staging reserve percentage.

Procedure

1. Click the **Data Management** > **File System** > **Configuration** tabs.
2. In the Options area, click **Edit**.
The Modify Settings dialog box is displayed.
3. In the Staging Reserve panel, click the **Enable** checkbox.
4. Enter a value in the **% of Total Space** text box.

This value represents the percentage of the total disk space to be reserved for disk staging, typically 20 to 30 percent.

5. Click **OK**.

Tape marker settings

Backup software from some vendors insert markers (tape markers, tag headers, or other names are used) in all data streams (both file system and VTL backups) sent to a Data Domain system.

Markers can significantly degrade data compression on a Data Domain system. As such, the default marker type auto is set and cannot be changed by the user. If this setting is not compatible with your backup software, contact your contracted support provider.

Note

For information about how applications work in a Data Domain environment, see *How EMC Data Domain Systems Integrate into the Storage Environment*. You can use these matrices and integration guides to troubleshoot vendor-related issues.

Fast copy operations

A fast copy operation clones files and directory trees of a source directory to a target directory on a Data Domain system.

The `force` option allows the destination directory to be overwritten if it exists. Executing the fast copy operation displays a progress status dialog box.

Note

A fast copy operation makes the destination equal to the source, but not at a specific time. There are no guarantees that the two are or were ever equal if you change either folder during this operation.

Performing a fast copy operation

Copy a file or directory tree from a Data Domain system source directory to another destination on the Data Domain system.

Procedure

1. Using the DD System Manager, click the **Data Management** > **File System** tabs and select **Fast Copy** from **More Tasks**.
The Fast Copy dialog box is displayed.
2. In the **Source** text box, enter the pathname of the directory where the data to be copied resides. For example, `/data/col1/backup/.snapshot/snapshot-name/dir1`.

Note

`col1` uses a lower case L followed by the number 1.

3. In the **Destination** text box, enter the pathname of the directory where the data will be copied to. For example, `/data/col1/backup/dir2`. This destination directory must be empty, or the operation fails.
 - If the Destination directory exists, click the checkbox **Overwrite existing destination if it exists**.

4. Click **OK**.
5. In the progress dialog box that appears, click **Close** to exit.

CHAPTER 6

MTrees

This chapter includes:

- [MTrees overview](#) 180
- [Monitoring MTree usage](#) 186
- [Managing MTree operations](#) 186

MTrees overview

An MTree is a logical partition of the Data Domain file system.

You can use MTrees in the following ways: for DD Boost storage units, VTL pools, or an NFS/CIFS share. MTrees allow granular management of snapshots, quotas, and Retention Lock. For systems that have DD Extended Retention and granular management of data migration policies from Active Tier to Retention Tier, MTree operations can be performed on a specific MTree as opposed to the entire file system.

Note

Although a Data Domain system supports a maximum of 100 MTrees, there is a smaller per-model number of MTrees that can be accessed by active read or write streams without risking rapid performance degradation.

- DD990, DD890, and DD880 platforms running DD OS 5.3, and later, support 32 currently accessible MTrees.
- DD4200, DD4500, and DD7200 platforms running DD OS 5.4, and later, support 32 currently accessible MTrees.
- All other platforms running DD OS 5.2 and DD OS 5.3, and later, support 14 currently accessible MTrees.
- The DD9500 platform supports 256 currently accessible MTrees. And, for a DD9500 system, you can have 540 MTree replication contexts (this is not true for other DD systems).

The degree of degradation depends on overall I/O intensity and other file system loads. For optimum performance, constrain the number of simultaneously active MTrees to a maximum of 14 or 32 as described above. Also, whenever possible, aggregate operations on the same MTree into a single operation.

There can be up to 99 MTrees designated for MTree replication contexts. For example, seven Data Domain systems, each with 14 active MTrees can replicate into a single Data Domain system.

Quotas

MTree quotas apply only to the logical data written to the MTree.

An administrator can set the storage space restriction for an MTree, Storage Unit, or VTL pool to prevent it from consuming excess space. There are two kinds of quota limits: hard limits and soft limits. You can set either a soft or hard limit or both a soft and hard limit. Both values must be integers, and the soft value must be less than the hard value.

When a soft limit is set, an alert is sent when the MTree size exceeds the limit, but data can still be written to it. When a hard limit is set, data cannot be written to the MTree when the hard limit is reached. Therefore, all write operations fail until data is deleted from the MTree.

See the section regarding MTree quota configuration for more information.

Quota enforcement

Enable or disable quota enforcement.

About the MTree overview panel

Lists all the active MTrees on the system and shows real-time data storage statistics. Information in the overview area is helpful in visualizing space usage trends.

Click the **Data Management** › **MTree** tabs.

- Click a checkbox of an MTree in the list to display details and perform configuration in the Summary view.
- Enter text (wildcards are supported) in the Filter By MTree Name field and click **Update** to list specific MTree names in the list.
- Delete filter text and click **Reset** to return to the default list.

Table 84 MTree overview information

Item	Description
MTree Name	The pathname of the MTree.
Quota Hard Limit	Percentage of hard limit quota used.
Quota Soft Limit	Percentage of hard limit quota used.
Last 24 Hr Pre-Comp (pre-compression)	Amount of raw data from the backup application that has been written in the last 24 hours.
Last 24 Hr Post-Comp (post-compression)	Amount of storage used after compression in the last 24 hours.
Last 24 hr Comp Ratio	The compression ratio for the last 24 hours.
Weekly Avg Post-Comp	Average amount of compressed storage used in the last five weeks.
Last Week Post-Comp	Average amount of compressed storage used in the last seven days.
Weekly Avg Comp Ratio	The average compression ratio for the last five weeks.
Last Week Comp Ratio	The average compression ratio for the last seven days.

About the summary view

View important file system statistics.

View detail information

Select an MTree to view details.

Table 85 MTree detail information for a selected MTree

Item	Description
Full Path	The pathname of the MTree.
Pre-Comp Used	The current amount of raw data from the backup application that has been written to the MTree.
Status	The current status of the MTree (combinations are supported). Status can be:

Table 85 MTree detail information for a selected MTree (continued)

Item	Description
	<ul style="list-style-type: none"> • D: Deleted • RO: Read-only • RW: Read/write • RD: Replication destination • RLCE: Retention Lock Compliance enabled • RLCD: Retention Lock Compliance disabled • RLGE: Retention Lock Governance enabled • RLGD: Retention Lock Governance disabled
Tenant Unit	Tenant-unit information displays if the selected MTree belongs to a tenant-unit. References to tenant-units display only when Secure Multi-tenancy is enabled.
Quota	
Quota Enforcement	Enabled or Disabled.
Pre-Comp Soft Limit	Current value. Click Configure to revise the quota limits.
Pre-Comp Hard Limit	Current value. Click Configure to revise the quota limits.
Quota Summary	Percentage of Hard Limit used.
Protocols	
CIFS Shared	<p data-bbox="790 1104 1166 1131">The CIFS share status. Status can be:</p> <ul style="list-style-type: none"> • Yes—The MTree or its parent directory is shared. • Partial—The subdirectory under this MTree is shared. • No—This MTree and its parent or child directories are not shared. <p data-bbox="790 1318 1198 1346">Click the CIFS link to go to the CIFS view.</p>
NFS Exported	<p data-bbox="790 1367 1166 1394">The NFS export status. Status can be:</p> <ul style="list-style-type: none"> • Yes—The MTree or its parent directory is exported. • Partial—The subdirectory under this MTree is exported. • No—This MTree and its parent or child directories are not exported. <p data-bbox="790 1581 1193 1608">Click the NFS link to go to the NFS view.</p>
DD Boost Storage Unit	<p data-bbox="790 1629 1225 1656">The DD Boost export status. Status can be:</p> <ul style="list-style-type: none"> • Yes—The MTree is exported. • No—This MTree is not exported. • Unknown—There is no information. <p data-bbox="790 1808 1305 1835">Click the DD Boost link to go to the DD Boost view.</p>
VTL Pool	If applicable, the name of the VTL pool that was converted to an MTree.

View MTree replication information

Display MTree replication configuration.

If the selected MTree is configured for replication, summary information about the configuration displays in this area. Otherwise, this area displays `No Record Found`.

- Click the [Replication](#) link to go to the Replication page for configuration and to see additional details.

Table 86 MTree replication information

Item	Description
Source	The source MTree pathname.
Destination	The destination MTree pathname.
Status	The status of the MTree replication pair. Status can be Normal, Error, or Warning.
Synced As Of Time	The last day and time the replication pair was synchronized.

View MTree snapshot information

If the selected MTree is configured for snapshots, summary information about the snapshot configuration displays.

- Click the **Snapshots** link to go to the Snapshots page to perform configuration or to see additional details.
- Click **Assign Snapshot Schedules** to assign a snapshot schedule to the selected MTree. Select the schedule's checkbox, and then click **OK** and **Close**. To create a snapshot schedule, click **Create Snapshot Schedule** (see the section about creating a snapshot schedule for instructions).

Table 87 MTree snapshot information

Item	Description
Total Snapshots	The total number of snapshots created for this MTree. A total of 750 snapshots can be created for each MTree.
Expired	The number of snapshots in this MTree that have been marked for deletion, but have not been removed with the clean operation as yet.
Unexpired	The number of snapshots in this MTree that are marked for keeping.
Oldest Snapshot	The date of the oldest snapshot for this MTree.
Newest Snapshot	The date of the newest snapshot for this MTree.
Next Scheduled	The date of the next scheduled snapshot.
Assigned Snapshot Schedules	The name of the snapshot schedule assigned to this MTree.

View MTree retention lock information

If the selected MTree is configured for one of the Retention Lock software options, summary information about the Retention Lock configuration displays.

Note

For information on how to manage Retention Lock for an MTree, see the section about working with DD retention lock.

Table 88 Retention lock information

Item	Description
Status	Indicates whether Retention Lock is enabled or disabled.
Retention Period	Indicates the minimum and maximum Retention Lock time periods.
UUID	Shows either: <ul style="list-style-type: none"> the unique identification number generated for an MTree when the MTree is enabled for Retention Lock that the Retention Lock on a file in the MTree has been reverted

Enabling and managing DD retention lock settings

Use the Retention Lock area of the GUI to modify retention lock periods.

Procedure

1. Click the **Data Management** > **MTree** > **Summary** tabs.
2. In the Retention Lock area, click **Edit**.
3. In the Modify Retention Lock dialog box, select **Enable** to enable Retention Lock on the Data Domain system.
4. Modify the minimum or maximum retention period (the feature must be enabled first), in the Retention Period panel.
5. Select an interval (minutes, hours, days, years). Click **Default** to show the default values.
6. Click **OK**.

Results

After you close the Modify Retention Lock dialog box, updated MTree information is displayed in the Retention Lock summary area.

About the space usage view (MTrees)

Display a visual representation of data usage for an MTree at certain points in time.

Click the **Data Management** > **MTree** > **Space Usage** tabs.

- Click a point on a graph line to display a box with data at that point.
- Click **Print** (at the bottom on the graph) to open the standard Print dialog box.
- Click **Show in new window** to display the graph in a new browser window.

The lines of the graph denote measurement for:

- **Pre-comp Written**—The total amount of data sent to the MTree by backup servers. Pre-compressed data on an MTree is what a backup server sees as the total uncompressed data held by an MTree-as-storage-unit, shown with the Space Used (left) vertical axis of the graph.

Note

For the MTrees Space Usage view, the system displays only pre-compressed information. Data can be shared between MTrees so compressed usage for a single MTree cannot be provided.

Checking Historical Space Usage

On the Space Usage graph, clicking an interval (that is, 7d, 30d, 60d, or 120d) on the Duration line above the graph allows you to change the number of days of data shown on the graph, from 7 to 120 days.

To see space usage for intervals over 120 days, issue the following command:

```
# fileysys show compression [summary | daily | daily-detailed] {[last n
{hours | days | weeks | months}] | [start date [end date]]}
```

About the daily written view (MTrees)

Display the flow of data over the last 24 hours. Data amounts are shown over time for pre- and post-compression.

It also provides totals for global and local compression amounts, and pre-compression and post-compression amounts.

- Click a point on a graph line to display a box with data at that point.
- Click **Print** (at the bottom on the graph) to open the standard Print dialog box.
- Click **Show in new window** to display the graph in a new browser window.

The lines on the graph denote measurements for:

- **Pre-Comp Written**—The total amount of data written to the MTree by backup servers. Pre-compressed data on an MTree is what a backup server sees as the total uncompressed data held by an MTree -as-storage-unit.
- **Post-Comp Written**—The total amount of data written to the MTree after compression has been performed, as shown in GiBs.
- **Total Comp Factor**—The total amount of compression the Data Domain system has performed with the data it received (compression ratio), shown with the Total Compression Factor (right) vertical axis of the graph.

Checking Historical Written Data

On the Daily Written graph, clicking an interval (that is, 7d, 30d, 60d, or 120d) on the Duration line above the graph allows you to change the number of days of data shown on the graph, from 7 to 120 days.

Below the Daily Written graph, the following totals display for the current duration value:

- Pre-Comp Written
- Post-Comp Written
- Global-Comp Factor
- Local-Comp Factor
- Total-Comp Factor

Monitoring MTree usage

Display space usage and data written trends for an MTree.

Procedure

1. Select a system in the Navigation panel.
2. Click the **Data Management** › **MTree** tabs.

The MTree view shows a list of configured MTrees, and when selected in the list, details of the MTree are shown in the Summary tab. The Space Usage and Daily Written tabs show graphs that visually display space usage amounts and data written trends for a selected MTree. The view also contains options that allow MTree configuration for CIFS, NFS, and DD Boost, as well as sections for managing snapshots and Retention Lock for an MTree.

The MTree view has an MTree overview panel and three tabs which are described in detail in these sections.

- [About the MTree overview panel on page 181](#)
- [About the summary view on page 181](#)
- [About the space usage view \(MTrees\) on page 184](#)
- [About the daily written view \(MTrees\) on page 185](#)

Managing MTree operations

This section describes MTree creation, configuration, how to enable and disable MTree quotas, and so on.

Creating an MTree

An MTree is a logical partition of the Data Domain file system. Use MTrees in for DD Boost storage units, VTL pools, or an NFS/CIFS share.

MTrees are created in the area `/data/col1/mtree_name`.

Procedure

1. Select a system in the Navigation panel.
2. Click the **Data Management** › **MTree** tabs.
3. In the MTree overview area, click **Create**.
4. Enter the name of the MTree in the MTree Name text box. MTree names can be up to 50 characters. The following characters are acceptable:
 - Upper- and lower-case alphabetical characters: A-Z, a-z
 - Numbers: 0-9
 - Embedded space
 - comma (,)
 - period (.), as long as it does not precede the name.
 - explanation mark (!)
 - number sign (#)

- dollar sign (\$)
 - per cent sign (%)
 - plus sign (+)
 - at sign (@)
 - equal sign (=)
 - ampersand (&)
 - semi-colon (;)
 - parenthesis [(and)]
 - square brackets ([and])
 - curly brackets ({and})
 - caret (^)
 - tilde (~)
 - apostrophe (unslanted single quotation mark)
 - single slanted quotation mark (')
5. Set storage space restrictions for the MTree to prevent it from consuming excessive space. Enter a soft or hard limit quota setting, or both. With a soft limit, an alert is sent when the MTree size exceeds the limit, but data can still be written to the MTree. Data cannot be written to the MTree when the hard limit is reached.

Note

The quota limits are pre-compressed values.
To set quota limits for the MTree, select **Set to Specific value** and enter the value.
Select the unit of measurement: MiB, GiB, TiB, or PiB.

Note

When setting both soft and hard limits, a quota's soft limit cannot exceed the quota's hard limit.

6. Click **OK**.
The new MTree displays in the MTree table.
-

Note

You may need to expand the width of the MTree Name column to see the entire pathname.

Configure and enable/disable MTree quotas

Set the storage space restriction for an MTree, Storage Unit, or VTL pool.

The **Data Management > Quota** page shows the administrator how many MTrees have no soft or hard quotas set. For MTrees with quotas set, the page shows the percentage of pre-compressed soft and hard limits used.

Consider the following information when managing quotas.

- MTree quotas apply to ingest operations. These quotas can be applied to data on systems that have the DD Extended Retention software, regardless of which tier it resides on, as well as VTL, DD Boost, CIFS, and NFS.
- Snapshots are not counted.
- Quotas cannot be set on the `/data/col1/backup` directory.
- The maximum quota value allowed is 4096 PiB.

Configure MTree quotas

Use the MTree tab or the Quota tab to configure MTree quotas.

Procedure

1. Select a system in the Navigation panel.
2. Select one of the following menu paths:
 - Click the **Data Management** › **MTree** tab.
 - Click the **Data Management** › **Quota** tab.
3. Select only one MTree in the MTree tab, or one or more MTrees in the Quota tab.

Note

Quotas cannot be set on the `/data/col1/backup` directory.

4. In the MTree tab, click the **Summary** tab, and then click the **Configure** button in the Quota area.
5. In the Quota tab, click the **Configure Quota** button.

Configuring MTree quotas

Enter values for hard and soft quotas and select the unit of measurement.

Procedure

1. In the Configure Quota for MTrees dialog box, enter values for hard and soft quotas and select the unit of measurement: MiB, GiB, TiB, or PiB.
2. Click **OK**.

Deleting an MTree

Removes the MTree from the MTree table. The MTree data is deleted at the next cleaning.

Note

Because the MTree and its associated data are not removed until file cleaning is run, you cannot create a new MTree with the same name as a deleted MTree until the deleted MTree is completely removed from the file system by the cleaning operation.

Procedure

1. Select a system in the Navigation panel.
2. Click the **Data Management** › **MTree** tabs.
3. Select an MTree.
4. In the MTree overview area, click **Delete**.
5. Click **OK** at the Warning dialog box.

- Click **Close** in the Delete MTree Status dialog box after viewing the progress.

Undeleting an MTree

Undelete retrieves a deleted MTree and its data and places it back in the MTree table.

An undelete of an MTree retrieves a deleted MTree and its data and places it back in the MTree table.

An undelete is possible only if file cleaning has not been run after the MTree was marked for deletion.

Note

You can also use this procedure to undelete a storage unit.

Procedure

- Select a system in the Navigation panel.
- Click the **Data Management** > **MTree** tabs.
- From the More Tasks menu, select **Undelete**.
- Select the checkboxes of the MTrees you wish to bring back and click **OK**.
- Click **Close** in the Undelete MTree Status dialog box after viewing the progress.

The recovered MTree displays in the MTree table.

Renaming an MTree

Use the Data Management MTree GUI to rename MTrees.

Procedure

- Select a system in the Navigation panel.
- Click the **Data Management** > **MTree** tabs.
- Select an MTree in the MTree table.
- Select the Summary tab.
- In the Detailed Information overview area, click **Rename**.
- Enter the name of the MTree in the New MTree Name text box.

See the section about creating an MTree for a list of allowed characters.

- Click **OK**.

The renamed MTree displays in the MTree table.

Replicating a system with quotas to one without

Replicate a Data Domain system with a DD OS that supports quotas, to a system with a DD OS that does not have quotas.

- A reverse resync, which takes the data from the system without quotas and puts it back in an MTree on the system that has quotas enabled (and which continues to have quotas enabled).
- A reverse initialization from the system without quotas, which takes its data and creates a new MTree on the system that supports quotas, but does not have quotas enabled because it was created from data on a system without quotas.

Note

Quotas were introduced as of DD OS 5.2.

CHAPTER 7

Snapshots

This chapter includes:

- [Snapshots overview](#)..... 192
- [Monitoring snapshots and their schedules](#)..... 193
- [Managing snapshots](#)..... 194
- [Managing snapshot schedules](#)..... 196
- [Recover data from a snapshot](#)..... 198

Snapshots overview

This chapter describes how to use the snapshot feature with MTree.

A snapshot saves a read-only copy (called a *snapshot*) of a designated MTree at a specific time. You can use a snapshot as a restore point, and you can manage MTree snapshots and schedules and display information about the status of existing snapshots.

Note

Snapshots created on the source Data Domain system are replicated to the destination with collection and MTree replication. It is not possible to create snapshots on a Data Domain system that is a replica for collection replication. It is also not possible to create a snapshot on the destination MTree of MTree replication. Directory replication does not replicate the snapshots, and it requires you to create snapshots separately on the destination system.

Snapshots for the MTree named `backup` are created in the system directory `/data/coll/backup/.snapshot`. Each directory under `/data/coll/backup` also has a `.snapshot` directory with the name of each snapshot that includes the directory. Each MTree has the same type of structure, so an MTree named `SantaClara` would have a system directory `/data/coll/SantaClara/.snapshot`, and each subdirectory in `/data/coll/SantaClara` would have a `.snapshot` directory as well.

Note

The `.snapshot` directory is not visible if only `/data` is mounted. When the MTree itself is mounted, the `.snapshot` directory is visible.

An expired snapshot remains available until the next file system cleaning operation.

The maximum number of snapshots allowed per MTree is 750. Warnings are sent when the number of snapshots per MTree reaches 90% of the maximum allowed number (from 675 to 749 snapshots), and an alert is generated when the maximum number is reached. To clear the warning, expire snapshots and then run the file system cleaning operation.

Note

To identify an MTree that is nearing the maximum number of snapshots, check the Snapshots panel of the MTree page regarding viewing MTree snapshot information.

Snapshot retention for an MTree does not take any extra space, but if a snapshot exists and the original file is no longer there, the space cannot be reclaimed.

Note

Snapshots and CIFS Protocol: As of DD OS 5.0, the `.snapshot` directory is no longer visible in the directory listing in Windows Explorer or DOS CMD shell. You can access the `.snapshot` directory by entering its name in the Windows Explorer address bar or the DOS CMD shell. For example, `\\dd\backup\.snapshot` or `Z:\.snapshot` when `Z:` is mapped as `\\dd\backup`).

Monitoring snapshots and their schedules

This section provides detailed and summary information about the status of snapshots and snapshot schedules.

About the snapshots view

The topics in this section describe the Snapshot view.

Snapshots overview panel

View the total number of snapshots, the number of expired snapshots, unexpired snapshots, and the time of the next cleaning.

Click the **Data Management** › **Snapshots** tabs.

Table 89 Snapshot overview panel information

Field	Description
Total Snapshots (Across all MTrees)	The total number of snapshots, active and expired, on all MTrees in the system.
Expired	The number of snapshots that have been marked for deletion, but have not been removed with the cleaning operation as yet.
Unexpired	The number of snapshots that are marked for keeping.
Next file system clean scheduled	The date the next scheduled file system cleaning operation will be performed.

Snapshots view

View snapshot information by name, by MTree, creation time, whether it is active, and when it expires.

The Snapshots tab displays a list of snapshots and lists the following information.

Table 90 Snapshot information

Field	Description
Selected Mtree	A drop-down list that selects the MTree the snapshot operates on.
Filter By	Items to search for in the list of snapshots that display. Options are: <ul style="list-style-type: none"> • Name—Name of the snapshot (wildcards are accepted). • Year—Drop-down list to select the year.
Name	The name of the snapshot image.
Creation Time	The date the snapshot was created.
Expires On	The date the snapshot expires.
Status	The status of the snapshot, which can be Expired or blank if the snapshot is active.

Schedules view

View the days snapshots will be taken, the times, the time they will be retained, and the naming convention.

Table 91 Snapshot schedule information

Field	Description
Name	The name of the snapshot schedule.
Days	The days the snapshots will be taken.
Times	The time of day the snapshots will be taken.
Retention Period	The amount of time the snapshot will be retained.
Snapshot Name Pattern	A string of characters and variables that translate into a snapshot name (for example, <code>scheduled-%Y-%m-%d-%H-%M</code> , which translates to “scheduled-2010-04-12-17-33”).

1. Select a schedule in the Schedules tab. The Detailed Information area appears listing the MTree(s) that share the same schedule with the selected MTree.
2. Click the **Add/Remove** button to add or remove MTree(s) from schedule list.

Managing snapshots

This section describes how to manage snapshots.

Creating a snapshot

Create a snapshot when an unscheduled snapshot is required.

Procedure

1. Click the **Data Management > Snapshots** tabs to open the Snapshots view.
2. In the Snapshots view, click **Create**.
3. In the Name text field, enter the name of the snapshot.
4. In the MTree(s) area, select a checkbox of one or more MTree(s) in the Available MTree(s) panel and click **Add**.
5. In the Expiration area, select one of these expiration options:
 - a. **Never Expire**.
 - b. Enter a number for the In text field, and select **Days, Weeks, Month, or Years** from the drop-down list. The snapshot will be retained until the same time of day as when it is created.
 - c. Enter a date (using the format `mm/dd/yyyy`) in the On text field, or click **Calendar** and click a date. The snapshot will be retained until midnight (00:00, the first minute of the day) of the given date.
6. Click **OK** and **Close**.

The snapshot is added to the list.

Modifying a snapshot expiration date

Modify snapshot expiration dates to remove them or extend their life for auditing or compliance.

Procedure

1. Click the **Data Management** > **Snapshots** tabs to open the Snapshots view.
 2. Click the checkbox of the snapshot entry in the list and click **Modify Expiration Date**. The Modify dialog box is displayed.
-

Note

More than one snapshot can be selected by clicking additional checkboxes.

3. In the Expiration area, select one of the following for the expiration date:
 - a. **Never Expire**.
 - b. In the In text field, enter a number and select **Days**, **Weeks**, **Month**, or **Years** from the drop-down list. The snapshot will be retained until the same time of day as when it is created.
 - c. In the On text field, enter a date (using the format *mm/dd/yyyy*) or click **Calendar** and click a date. The snapshot will be retained until midnight (00:00, the first minute of the day) of the given date.
4. Click **OK**.

Renaming a snapshot

Use the Snapshot tab to rename a snapshot.

Procedure

1. Click the **Data Management** > **Snapshots** tabs to open the Snapshots view.
2. Select the checkbox of the snapshot entry in the list and click **Rename**.
3. In the Name text field, enter a new name.
4. Click **OK**.

Expiring a snapshot

Snapshots cannot be deleted. To release disk space, expire snapshots and they will be deleted in the next cleaning cycle after the expiry date.

Procedure

1. Click the **Data Management** > **Snapshots** tabs to open the Snapshots view.
 2. Click the checkbox next to snapshot entry in the list and click **Expire**.
-

Note

More than one snapshot can be selected by selecting additional checkboxes. The snapshot is marked as Expired in the Status column and will be deleted at the next cleaning operation.

Managing snapshot schedules

Set up and manage a series of snapshots that will be automatically taken at regular intervals (a snapshot schedule).

Multiple snapshot schedules can be active at the same time.

Note

If multiple snapshots are scheduled to occur at the same time, only one is retained. Which one is retained is indeterminate, thus only one snapshot should be scheduled for a given time.

Creating a snapshot schedule

Create a weekly or monthly snapshot schedule using the Data Management GUI.

Procedure

1. Click the **Data Management** > **Snapshots** > **Schedules** tabs to open the Schedules view.
2. Click **Create**.
3. In the **Name** text field, enter the name of the schedule.
4. In the **Snapshot Name Pattern** text box, enter a name pattern.
 Enter a string of characters and variables that translates to a snapshot name (for example, `scheduled-%Y-%m-%d-%H-%m`, translates to "scheduled-2012-04-12-17-33"). Use alphabetic characters, numbers, `_`, `-`, and variables that translate into current values.
5. Click **Validate Pattern & Update Sample**.
6. Click **Next**.
7. Select the date when the schedule will be executed:
 - a. **Weekly**—Click checkboxes next to the days of the week or select **Every Day**.
 - b. **Monthly**—Click the **Selected Days** option and click the dates on the calendar, or select the **Last Day of the Month** option.
 - c. Click **Next**.
8. Select the time of day when the schedule will be executed:
 - a. **At Specific Times**—Click **Add** and in the Time dialog that appears, enter the time in the format `hh:mm`, and click **OK**.
 - b. **In Intervals**—Click the drop-down arrows to select the start and end time `hh:mm` and AM or PM. Click the **Interval** drop-down arrows to select a number and then the hours or minutes of the interval.
 - c. Click **Next**.
9. In the Retention Period text entry field, enter a number and click the drop-down arrow to select days, months, or years, and click **Next**.
 Schedules must explicitly specify a retention time.
10. Review the parameters in the schedule summary and click **Finish** to complete the schedule or **Back** to change any entries.

11. If an MTree is not associated with the schedule, a warning dialog box asks if you would like to add an MTree to the schedule. Click **OK** to continue (or **Cancel** to exit).
12. To assign an MTree to the schedule, in the MTree area, click the checkbox of one or more MTrees in the Available MTrees panel, then click **Add** and **OK**.

Naming conventions for snapshots created by a schedule

The naming convention for scheduled snapshots is the word `scheduled` followed by the date when the snapshot is to occur, in the format `scheduled-yyyy-mm-dd-hh-mm`. For example, `scheduled-2009-04-27-13-30`.

The name “`mon_thurs`” is the name of a snapshot schedule. Snapshots generated by that schedule might have the names `scheduled-2008-03-24-20-00`, `scheduled-2008-03-25-20-00`, etc.

Modifying a snapshot schedule

Change the snapshot schedule name, date, and retention period.

Procedure

1. In the schedule list, select the schedule and click **Modify**.
2. In the Name text field, enter the name of the schedule and click **Next**.
Use alphanumeric characters, and the `_` and `-`.
3. Select the date when the schedule is to be executed:
 - a. **Weekly**—Click checkboxes next to the days of the week or select **Every Day**.
 - b. **Monthly**—Click the **Selected Days** option and click the dates on the calendar, or select the **Last Day of the Month** option.
 - c. Click **Next**.
4. Select the time of day when the schedule is to be executed:
 - a. **At Specific Times**—Click the checkbox of the scheduled time in the Times list and click **Edit**. In the Times dialog that appears, enter a new time in the format `hh:mm`, and click **OK**. Or click **Delete** to remove the scheduled time.
 - b. **In Intervals**—Click the drop-down arrows to select the start and end time `hh:mm` and AM or PM. Click the Interval drop-down arrows to select a number and then the hours or minutes of the interval.
 - c. Click **Next**.
5. In the Retention Period text entry field, enter a number and click the drop-down arrow to select days, months, or years, and click **Next**.
6. Review the parameters in the schedule summary and click **Finish** to complete the schedule or **Back** to change any entries.

Deleting a snapshot schedule

Delete a snapshot schedule from the schedule list.

Procedure

1. In the schedule list, click the checkbox to select the schedule and click **Delete**.
2. In the verification dialog box, click **OK** and then **Close**.

Recover data from a snapshot

Use the fastcopy operation to retrieve data stored in a snapshot. See the section regarding fast copy operations.

CHAPTER 8

CIFS

This chapter includes:

- [CIFS overview](#) 200
- [Configuring SMB signing](#) 200
- [Performing CIFS setup](#) 202
- [Working with shares](#) 204
- [Managing access control](#) 210
- [Monitoring CIFS operation](#) 214
- [Performing CIFS troubleshooting](#) 217

CIFS overview

Common Internet File System (CIFS) clients can have access to the system directories on the Data Domain system.

- The `/data/coll/backup` directory is the destination directory for compressed backup server data.
- The `/ddvar/core` directory contains Data Domain System core and log files (remove old logs and core files to free space in this area).

Note

You can also delete core files from the `/dvar` or the `/ddvar/ext` directory if it exists.

Clients, such as backup servers that perform backup and restore operations with a Data Domain System, at the least, need access to the `/data/coll/backup` directory. Clients that have administrative access need to be able to access the `/ddvar/core` directory to retrieve core and log files.

As part of the initial Data Domain system configuration, CIFS clients were configured to access these directories. This chapter describes how to modify these settings and how to manage data access using the Data DD Manager and the `cifs` command.

Note

- The DD System Manager **Data Management** > **CIFS** page allows you to perform major CIFS operations such as enabling and disabling CIFS, setting authentication, managing shares, and viewing configuration and share information.
 - The `cifs` command contains all the options to manage CIFS backup and restores between Windows clients and Data Domain systems, and to display CIFS statistics and status. For complete information about the `cifs` command, see the *EMC Data Domain Operating System Command Reference Guide*.
 - For information about the initial system configuration, see the *EMC Data Domain Operating System Initial Configuration Guide*.
 - For information about setting up clients to use the Data Domain system as a server, see the related tuning guide, such as the *CIFS Tuning Guide*, which is available from the support.emc.com web site. Search for the complete name of the document using the Search EMC Support field.
-

Configuring SMB signing

On a DD OS version that supports it, you can configure the SMB signing feature using the CIFS option called server signing.

This feature is disabled by default because it degrades performance. When enabled, SMB signing can cause a 29 percent (reads) to 50 percent (writes) throughput performance drop, although individual system performance will vary. There are three possible values for SMB signing: disabled, auto and mandatory:

- When SMB signing is set to disabled, SMB signing is disabled, this is the default.

- When SMB signing is set to auto, SMB signing is offered, but not enforced.
- When SMB signing is set to mandatory, SMB signing is required, and both computers in the SMB connection must have SMB signing enabled.

SMB Signing CLI Commands

```
cifs option set "server signing" auto
```

Sets server signing to auto.

```
cifs option set "server signing" mandatory
```

Sets server signing to mandatory.

```
cifs option reset "server signing"
```

Resets server signing to the default (disabled).

As a best practice, whenever you change the SMB signing options, disable and then enable (restart) CIFS service using the following CLI commands:

```
cifs disable
```

```
cifs enable
```

The System Manager interface now displays whether the SMB signing option is disabled or set to auto or mandatory. To view this setting in the interface, navigate to: **Data Management** > **CIFS** > **Configuration tab**. In the Options area, the value for the SMB signing option will be disabled, auto or mandatory reflecting the value set using the CLI commands.

Figure 6 SMB Signing Option

The screenshot shows the System Manager interface for CIFS configuration. The 'Data Management' tab is selected, and the 'CIFS' sub-tab is active. The 'CIFS Status' section shows 'CIFS is enabled and running.' with a 'Disable' button. The 'Connections' section shows 'Open Connections: 0' and 'Open Files: 0'. The 'Configuration' section includes 'Authentication' and 'Options' tabs. The 'Options' section is expanded, showing a table of CIFS options. The 'server signing' option is highlighted with a red box and has a value of 'auto'.

Option	Value
idmap-type	rid
server signing	auto
nfs-acs	enabled
allowtrusteddomains	enabled
loglevel	1
maxxmit	65536
restrict-anonymous	disabled
smbd-mem-limit	209715200

Performing CIFS setup

This section contains instructions about enabling CIFS services, naming the CIFS server, and so on.

Preparing clients for access to data domain systems

Find EMC documentation online.

Procedure

1. Log into the EMC Online Support (support.emc.com) web site.
2. In the Search EMC Support field, enter the name of the document that you are looking for.
3. Select the appropriate document, such as the *CIFS and Data Domain Systems Tech Note*.
4. Follow the instructions in the document.

Enabling CIFS services

Enable the client to access the system using the CIFS protocol.

After configuring a client for access to Data Domain systems, enable CIFS services, which allows the client to access the system using the CIFS protocol.

Procedure

1. For the Data Domain system that is selected in the DD System Manager Navigation tree, click **Data Management > CIFS**.
2. In the CIFS Status area, click **Enable**.

Naming the CIFS server

The hostname for the Data Domain system that serves as the CIFS server is set during the system's initial configuration.

To change a CIFS server name, see the procedures in the section regarding setting authentication parameters.

A Data Domain system's hostname should match the name assigned to its IP address, or addresses, in the DNS table. Otherwise authentication, as well as attempts to join a domain, can fail. If you need to change the Data Domain system's hostname, use the `net set hostname` command, and also modify the system's entry in the DNS table.

When the Data Domain system acts as a CIFS server, it takes the hostname of the system. For compatibility purposes, it also creates a NetBIOS name. The NetBIOS name is the first component of the hostname in all uppercase letters. For example, the hostname `jp9.oasis.local` is truncated to the NetBIOS name `JP9`. The CIFS server responds to both names.

You can have the CIFS server respond to different names at the NetBIOS levels by changing the NetBIOS hostname.

Changing the NetBIOS hostname

Change the NetBIOS hostname with the CLI.

Procedure

1. Display the current NetBIOS name by entering:

```
# cifs show config
```

2. Use the

```
cifs set nb-hostname nb-hostname
command.
```

Setting authentication parameters

Set the Data Domain authentication parameters for working with CIFS.

Click the Configure link in to the left of the Authentication label in the Configuration tab. The system will navigate to the **System Settings** > **Access Management** > **Authentication** tab where you can configure authentication for Active Directory, Kerberos, Workgroups, and NIS.

Specifying a WINS server

From the CLI, the WINS server can be set when the Data Domain system needs to join a NT4 domain.

This option does not need to be set for the active directory domain or workgroup authentication.

Procedure

- Use this command:
- ```
cifs set wins-server ipaddr
```

.

---

### Note

If CIFS clients are using NetBIOS, a WINS server may be needed to resolve NetBIOS names to IP addresses.

---

## Restricting CIFS interfaces

By default, the CIFS server listens on all Data Domain system NIC-active interfaces.

From the CLI:

### Procedure

- Use this command:
- ```
cifs option set interfaces value
```

.

Results

The *value* is a list of interfaces, such as Ethernet port names. Multiple interfaces must be separated by a space and enclosed within double quotation marks, for example, "**eth0a eth9b**".

Setting CIFS options

View CIFS configuration, restrict anonymous connections.

Procedure

1. Select the Data Domain system in the Navigation tree and click the **Data Management > CIFS > Configuration** tabs.
2. In the Options area, click **Configure Options**.

The Configure Options dialog box is displayed.

3. To restrict anonymous connections, click the checkbox of the **Enable** option in the Restrict Anonymous Connections area.
4. In the LogLevel area, click the drop-down list to select the level number.

The level is an integer from 0 (zero) to 10 (ten). One is the default system level that sends the least-detailed level of CIFS-related log messages, ten results in the most detail. Log messages are located in the files `/ddvar/log/debug/cifs/clients.log` and `/ddvar/log/debug/cifs/cifs.log`.

Note

A log level of 10 degrades system performance. Click the **Default** in the Log Level area after debugging an issue. This sets the level back to 1.

Disabling CIFS services

Prevent clients from accessing the Data Domain system.

Procedure

1. Select the Data Domain system in the Navigation tree and click the **Data Management > CIFS** tabs.
2. In the Status area, click **Disable**.

The Disable CIFS dialog box is displayed.

3. Click **OK**.

Even after disabling CIFS access, CIFS authentication services continue to run on the Data Domain system. This continuation is required to authenticate active directory domain users for management access.

Working with shares

To share data, create shares on the Data Domain system.

Shares are administered on the Data Domain system and the CIFS systems.

Creating shares on the Data Domain system

When creating shares, you have to assign client access to each directory separately and remove access from each directory separately. For example, a client can be removed from `/ddvar` and still have access to `/data/col1/backup`

A Data Domain system supports a maximum number of 3000 CIFS shares.¹ And 600 simultaneous connections are allowed.

Note

If Replication is to be implemented, a Data Domain system can receive backups from both CIFS clients and NFS clients as long as separate directories are used for each. Do not mix CIFS and NFS data in the same directory.

Procedure

1. From the Navigation panel, select a Data Domain system to configure shares.
2. Click **Data Management** > **CIFS** tabs to navigate to the CIFS view.
3. Ensure authentication has been configured, as described in the section regarding setting authentication parameters.
4. On the CIFS client, set shared directory permissions or security options.
5. On the CIFS view, click the Shares tab.
6. Click **Create**.

The Create Shares dialog box is displayed.

7. In the Create Shares dialog box, enter the following information:

Table 92 Shares dialog box information

Item	Description
Share Name	A descriptive name for the share.
Directory Path	The path to the target directory (for example, <code>/data/col1/backup/dir1</code>).
	<hr/> <p>Note</p> <p>col1 uses the lower case letter L followed by the number 1.</p> <hr/>
Comment	A descriptive comment about the share.

Note

The share name can be a maximum of 80 characters and cannot contain the following characters: `\ / : * ? " < > | + [] ; , =` or extended ASCII characters.

8. Add a client by clicking Add (+) in the Clients area. The Client dialog box appears. Enter the name of the client in the Client text box and click **OK**.

Consider the following when entering the client name.

1. May be affected by hardware limitations.

- No blanks or tabs (white space) characters are allowed.
- It is not recommended to use both an asterisk (*) and individual client name or IP address for a given share. When an asterisk (*) is present, any other client entries for that share are not used.
- It is not required to use both client name and client IP address for the same client on a given share. Use client names when the client names are defined in the DNS table.
- To make share available to all clients, specify an asterisk (*) as the client. 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.

Repeat this step for each client that you need to configure.

9. In the Max Connections area, select the text box and enter the maximum number of connections to the share that are allowed at one time. The default value of zero (also settable via the Unlimited button) enforces no limit on the number of connections.
10. Click **OK**.

The newly created share appears at the end of the list of shares, located in the center of the Shares panel.

Modifying a share on a Data Domain system

Change share information and connections.

Procedure

1. In the Shares tab, click the checkbox next the share that you wish to modify in the Share Name list.
2. Click **Modify**.
The Modify Share dialog box appears.
3. Modify share information:
 - a. To change the comment, enter new text in the Comment text field.
 - b. To modify a User or Group names, in the User/Group list, click the checkbox of the user or group and click **Edit** (pencil icon) or **Delete** (X). To add a user or group, click (+), and in the User/Group dialog box select the Type for User or Group, and enter the user or group name.
 - c. To modify a client name, in the Client list click the checkbox of the client and click **Edit** (pencil icon) or **Delete** (X). To add a client, click the Add (+) and add the name in the Client dialog box.

Note

To make the share available to all clients, specify an asterisk (*) as the client. 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.

- d. Click **OK**.
4. In the Max Connections area, in the text box, change the maximum number of connections to the share that are allowed at one time. Or select Unlimited to enforce no limit on the number of connections.

5. Click **OK**.

Creating a share from an existing share

Create a share from an existing share and modify the new share if necessary.

Note

User permissions from the existing share are carried over to the new share.

Procedure

1. In the CIFS Shares table, click the checkbox of the share you wish to use as the source.
2. Click **Create From**.
The Create From Existing Share dialog box appears.
3. Modify the share information, as described in the section about modifying a share on a Data Domain system.

Disabling a share on a Data Domain system

Disable one or more existing shares.

Procedure

1. In the Shares tab, click the checkbox of the share you wish to disable in the Share Name list.
2. Click **Disable**.
The Disable Shares Status dialog box appears.
3. Click **Close**.

Enabling a share on a Data Domain system

Enable one or more existing shares.

Procedure

1. In the Shares tab, click the checkbox of the shares you wish to enable in the Share Name list.
2. Click **Enable**.
The Enable Shares Status dialog box appears.
3. Click **Close**.

Deleting a share on a Data Domain system

Delete one or more existing shares.

Procedure

1. In the Shares tab, click the checkbox of the shares you wish to delete in the Share Name list.
2. Click **Delete**.
The Warning dialog box appears.

3. Click **OK**.

The shares are removed.

Performing MMC administration

Use the Microsoft Management Console (MMC) for administration.

DD OS supports these MMC features:

- Share management, except for browsing when adding a share, or the changing of the offline settings default, which is a manual procedure.
- Session management.
- Open file management, except for deleting files.

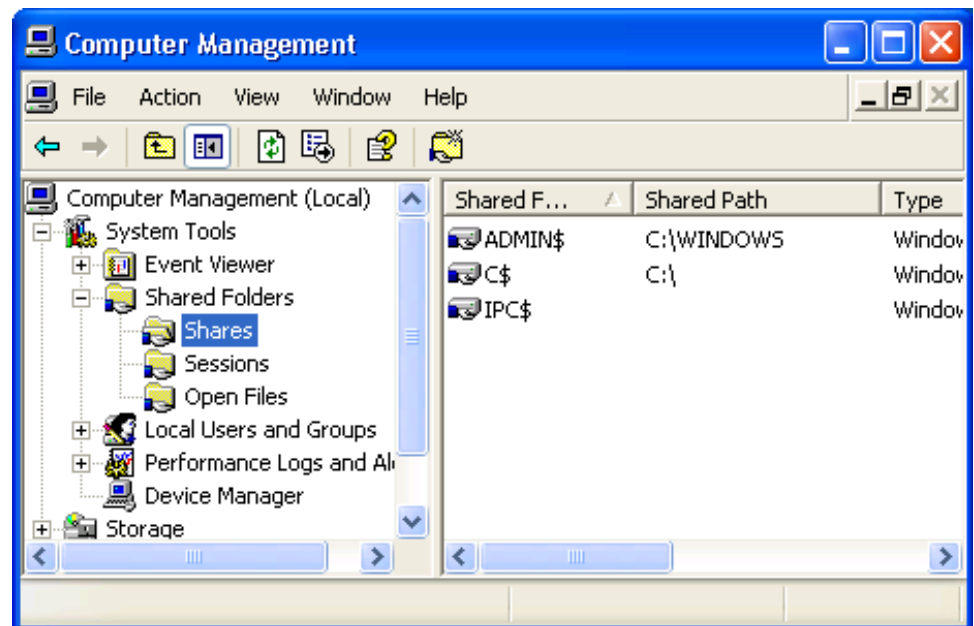
Connecting to a Data Domain system from a CIFS client

Use CIFS to connect to a Data Domain system and create a read-only backup subfolder.

Procedure

1. On the Data Domain system CIFS page, verify that CIFS Status shows that CIFS is enabled and running.
2. In the Control Panel, open Administrative Tools and select **Computer Management**.
3. In the Computer Management dialog box, right-click **Computer Management (Local)** and select **Connect to another computer** from the menu.
4. In the Select Computer dialog box, select **Another computer** and enter the name or IP address for the Data Domain system.
5. Create a `\backup` subfolder as read-only. For more information, see the section on creating a `/data/col1/backup` subfolder as read-only.

Figure 7 Computer Management dialog box



Creating a \data\col1\backup subfolder as read-only

Enter a path, share name, and select permissions.

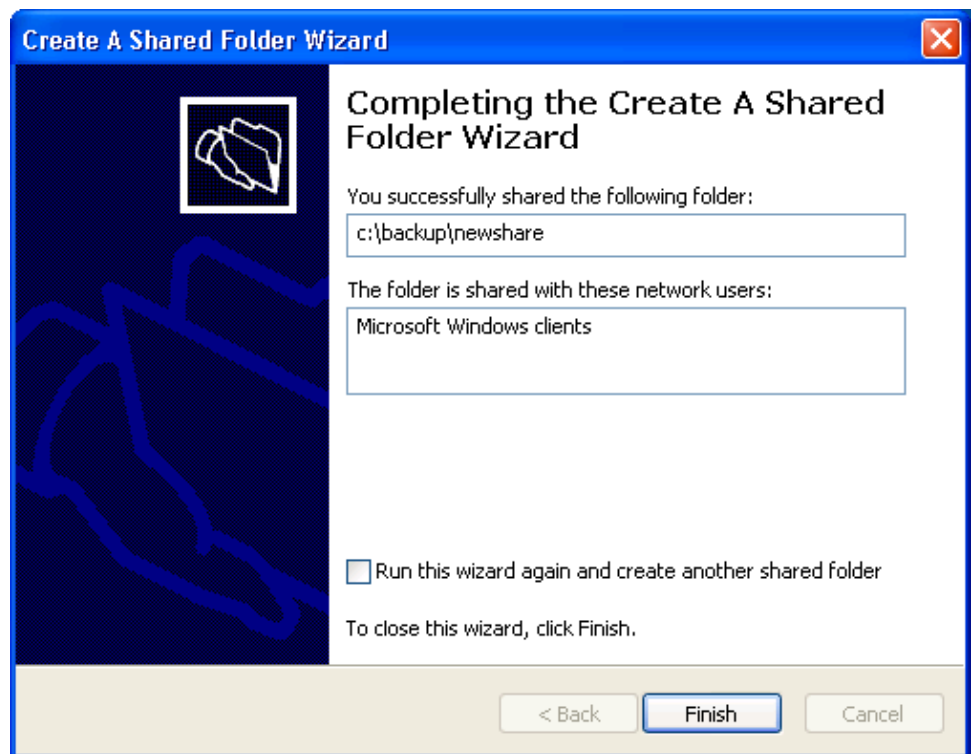
Procedure

1. In the Control Panel, open Administrative Tools and select **Computer Management**.
2. Right-click **Shares** in the Shared Folders directory.
3. Select **New File Share** from the menu.

The **Create a Shared Folder** wizard opens. The computer name should be the name or IP address of the Data Domain system.

4. Enter the path for the Folder to share, for example, enter C:\data\col1\backup\newshare.
5. Enter the Share name, for example, enter **newshare**. Click **Next**.
6. For the Share Folder Permissions, selected Administrators have full access. Other users have read-only access. Click **Next**.

Figure 8 Completing the Create a Shared Folder Wizard



7. The Completing dialog shows that you have successfully shared the folder with all Microsoft Windows clients in the network. Click **Finish**.

The newly created shared folder is listed in the Computer Management dialog box.

Displaying CIFS information

Display information about shared folders, sessions, and open files.

Procedure

1. In the Control Panel, open Administrative Tools and select **Computer Management**.
2. Select one of the Shared Folders (**Shares**, **Sessions**, or **Open Files**) in the System Tools directory.

Information about shared folders, sessions, and open files is shown in the right panel.

Managing access control

Access shared from a Windows client, provide administrative access, and allow access from trusted domain users.

Accessing shares from a Windows client

Use the command line to map a share.

Procedure

- From the Windows client use this DOS command:

```
net use drive: backup-location
```

For example, enter:

```
# \\dd02\backup /USER:dd02\backup22
```

This command maps the backup share from Data Domain system dd02 to drive H on the Windows system and gives the user named backup22 access to the \\DD_sys\backup directory.

Providing domain users administrative access

Use the command line to add CIFS and include the domain name in the ssh instruction.

Procedure

- Enter: `adminaccess authentication add cifs`

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

```
C:> ssh "domain2\djones" @dd22
```

Allowing access from trusted domain users

You do not need to set this option because trusted domain users are always allowed to access shares from the Data Domain system.

Procedure

- Enter: `cifs option set allowtrusteddomains enabled`

To disable access from trusted domain users, substitute `disabled` for `enabled`.

Note

These are domains that are trusted by the domain that includes the Data Domain system.

Allowing administrative access to a Data Domain system for domain users

Use the command line to map a DD system default group number, and then enable CIFS administrative access.

Procedure

1. To map a Data Domain System default group number to a Windows group name that differs from the default group name, use the `cifs option set "dd admin group2" ["windows grp-name"]` command.

The Windows group name is a group (based on one of the user roles—admin, user, or back-up operator) that exists on a Windows domain controller.

Note

For a description of DD OS user roles and Windows groups, see the section about managing Data Domain systems.

2. Enable CIFS administrative access by entering:

```
adminaccess authentication add cifs
```

- The default Data Domain System group `dd admin group1` is mapped to the Windows group `Domain Admins`.
- You can map the default Data Domain System group `dd admin group2` to a Windows group named `Data Domain` that you create on a Windows domain controller.
- Access is available through SSH, Telnet, FTP, HTTP, and HTTPS.
- After setting up administrative access to the Data Domain system from the Windows group `Data Domain`, you must enable CIFS administrative access using the `adminaccess` command.

Restricting administrative access from Windows

Use the command line to prohibit access to users without a DD account.

Procedure

- Enter:

```
adminaccess authentication del cifs
```

This command prohibits Windows users access to the Data Domain system if they do not have an account on the Data Domain system.

File access

This sections contains information about ACLs, setting DACL and SACL permissions using Windows Explorer, and so on.

NT access control lists

Access control lists (ACLs) are enabled by default on the Data Domain system.

Note

When CIFS ACLs are disabled using the command `cifs option set ntfs-acls disabled`, the Data Domain system generates an ACL that approximates the UNIX permissions, whether or not there were previously set CIFS ACLs. For more detailed information about ACLs, see your Windows Operating System documentation.

CAUTION

Data Domain recommends that you do not disable NTFS ACLs once they have been enabled. Contact Data Domain Support prior to disabling NTFS ACLs.

Default ACL Permissions

The default permissions, which are assigned to new objects created through the CIFS protocol when ACLs are enabled, depend on the status of the parent directory. There are three different possibilities:

- The parent directory has no ACL because it was created through NFS protocol.
- The parent directory has an inheritable ACL, either because it was created through the CIFS protocol or because ACL had been explicitly set. The inherited ACL is set on new objects.
- The parent directory has an ACL, but it is not inheritable. The permissions are as follows:

Table 93 Permissions

Type	Name	Permission	Apply To
Allow	SYSTEM	Full control	This folder only
Allow	CREATOR OWNER	Full control	This folder only

Note

CREATOR OWNER is replaced by the user creating the file/folder for normal users and by Administrators for administrative users.

Permissions for a New Object when the Parent Directory Has No ACL

The permissions are as follows:

- BUILTIN\Administrators:(OI)(CI)F
- NT AUTHORITY\SYSTEM:(OI)(CI)F
- CREATOR OWNER:(OI)(CI)(IO)F
- BUILTIN\Users:(OI)(CI)R
- BUILTIN\Users:(CI)(special access:)FILE_APPEND_DATA
- BUILTIN\Users:(CI)(IO)(special access:)FILE_WRITE_DATA
- Everyone:(OI)(CI)R

These permissions are described in more detail as follows:

Table 94 Permissions Detail

Type	Name	Permission	Apply To
Allow	Administrators	Full control	This folder, subfolders, and files
Allow	SYSTEM	Full control	This folder, subfolders, and files
Allow	CREATOR OWNER	Full control	Subfolders and files only
Allow	Users	Read & execute	This folder, subfolders, and files
Allow	Users	Create subfolders	This folder and subfolders only
Allow	Users	Create files	Subfolders only
Allow	Everyone	Read & execute	This folder, subfolders, and files

Setting ACL Permissions and Security

Windows-based backup and restore tools such as NetBackup can be used to back up DACL- and SACL-protected files to the Data Domain system, and to restore them from the Data Domain system.

Granular and Complex Permissions (DACL)

You can set granular and complex permissions (DACL) on any file or folder object within the DDFS file systems, either through using Windows commands such as `cacls`, `xcaccls`, `xcopy` and `scopy`, or through the CIFS protocol using the Windows Explorer GUI.

Audit ACL (SACL)

You can set audit ACL (SACL) on any object in the Data Domain File System (DDFS), either through commands or through the CIFS protocol using the Windows Explorer GUI.

Setting DACL permissions using the Windows Explorer

Use Explorer properties settings to select DACL permissions.

Procedure

1. Right-click the file or folder and select **Properties**.
2. In the Properties dialog box, click the Security tab.
3. Select the group or user name, such as **Administrators**, from the list. The permissions appear, in this case for `Administrators`, `Full Control`.
4. Click the **Advanced** button, which enables you to set special permissions.
5. In the Advanced Security Settings for ACL dialog box, click the Permissions tab.
6. Select the permission entry in the list.
7. To view more information about a permission entry, select the entry and click **Edit**.
8. Select the Inherit from parent option to have the permissions of parent entries inherited by their child objects, and click **OK**.

Setting SACL permissions using the Windows Explorer

Use Explorer properties settings to select SACL permissions.

Procedure

1. Right-click the file or folder and select **Properties** from the menu.
2. In the Properties dialog box, click the Security tab.
3. Select the group or user name, such as **Administrators**, from the list, which displays its permissions, in this case, `Full Control`.
4. Click the **Advanced** button, which enables you to set special permissions.
5. In the Advanced Security Settings for ACL dialog box, click the Auditing tab.
6. Select the auditing entry in the list.
7. To view more information about special auditing entries, select the entry and click **Edit**.
8. Select the Inherit from parent option to have the permissions of parent entries inherited by their child objects, and click **OK**.

Viewing or changing the current owner security ID (owner SID)

Use the Advanced Security Settings for ACL dialog box.

Procedure

1. In the Advanced Security Settings for ACL dialog box, click the Owner tab.
2. To change the owner, select a name from the Change owner list, and click **OK**.

Controlling ID account mapping

The CIFS option `idmap-type` controls ID account mapping behavior.

This option has two values: `rid` (the default) and `none`. When the option is set to `rid`, the ID-to-id mapping is performed internally. When the option is set to `none`, all CIFS users are mapped to a local UNIX user named “`cifsuser`” belonging to the local UNIX group `users`.

Consider the following information while managing this option.

- CIFS must be disabled to set this option. If CIFS is running, disable CIFS services.
- The `idmap-type` can be set to `none` only when ACL support is enabled.
- Whenever the `idmap` type is changed, a file system metadata conversion might be required for correct file access. Without any conversion, the user might not be able to access the data. To convert the metadata, consult your contracted support provider.

Monitoring CIFS operation

Monitoring CIFS Operation topics.

Displaying CIFS status

View and enable/disable CIFS status.

Procedure

1. In the DD System Manager, select **Data Management > CIFS**.

2.
 - Status is either enabled and running, or disabled but CIFS authentication is running.
To enable CIFS, see the section regarding enabling CIFS services. To disable CIFS, see the section regarding disabling CIFS services.
 - **Connections** lists the tally of open connections and open files.
Click **Connection Details** to see more connection information.
 - Shares information is described in the section regarding displaying shares information.

Display CIFS configuration

This section displays CIFS Configuration.

Authentication configuration

The information in the Authentication panel changes, depending on the type of authentication that is configured.

Active directory configuration

Table 95 Active directory configuration information

Item	Description
Mode	The Active Directory mode displays.
Realm	The configured realm displays.
DDNS	The status of the DDNS Server displays: either enabled or disabled.
Domain Controllers	The name of the configured domain controllers display or a * if all controllers are permitted.
Organizational Unit	The name of the configured organizational units displays.
CIFS Server Name	The name of the configured CIFS server displays.
WINS Server Name	The name of the configured WINS server displays.
Short Domain Name	The short domain name displays.

Workgroup configuration

Table 96 Workgroup configuration authentication information

Item	Description
Mode	The Workgroup mode displays.
Workgroup Name	The configured workgroup name displays.
DDNS	The status of the DDNS Server displays: either enabled or disabled.
CIFS Server Name	The name of the configured CIFS server displays.
WINS Server Name	The name of the configured WINS server displays.

Display shares information

This section displays shares information.

Viewing configured shares

View the list of configured shares.

Table 97 Configured shares information

Item	Description
Share Name	The name of the share (for example, share1).
Share Status	The status of the share: either enabled or disabled.
Directory Path	The directory path to the share (for example, /data/col1/backup/dir1).
<p>Note</p> <p>col1 uses the lower case letter L followed by the number 1.</p>	
Directory Path Status	The status of the directory path.

- To list information about a specific share, enter the share name in the Filter by Share Name text box and click **Update**.
- Click **Update** to return to the default list.
- To page through the list of shares, click the ◀ and ▶ arrows at the bottom right of the view to page forward or backward. To skip to the beginning of the list, click ⌊ and to skip to the end, click ⌋.
- Click the **Items per Page** drop-down arrow to change the number of share entries listed on a page. Choices are 15, 30, or 45 entries.

Viewing detailed share information

Display detailed information about a share by clicking a share name in the share list.

Table 98 Share information

Item	Description
Share Name	The name of the share (for example, share1).
Directory Path	The directory path to the share (for example, /data/col1/backup/dir1).
<p>Note</p> <p>col1 uses the lower case letter L followed by the number 1.</p>	
Comment	The comment that was configured when the share was created.
Share Status	The status of the share: either enabled or disabled.
Number of ACE's	The number of Access Control Entries.

- The Clients area lists the clients that are configured to access the share, along with a client tally beneath the list.

- The User/Groups area lists the names and type of users or groups that are configured to access the share, along with a user or group tally beneath the list.
- The Options area lists the name and value of configured options.

Displaying CIFS statistics

Use the command line to display CIFS statistics.

Procedure

- Enter: `cifs show detailed-stats`

The output shows number of various SMB requests received and the time taken to process them.

Performing CIFS troubleshooting

This section provides basic troubleshooting procedures.

Note

The `cifs troubleshooting` commands provide detailed information about CIFS users and groups.

Displaying clients current activity

Use the command line to display shares accessed from clients, data transfer information, and information about locked files.

Procedure

- Enter: `cifs show active`

Results

The output shows shares accessed from a client system, the current data transfer, and locked files.

Table 99 Shares accessed from client

PID	Username	Group	Machine
568	sysadmin	admin	svr24 (192.168.1.5)
566	sysadmin	admin	svr22 (192.168.1.6)

Table 100 Data transfer information

Services	PID	Machine	Connected at
ddvar	566	server22	Tues Jan 13 12:11:03 2009
backup	568	server24	Tues Jan 13 12:09:44 2009

The output for locked files provides the following information by file name or date.

Table 101 Locked files information

PID	Deny mode	Access	Read/Write	Oplock
566	DENY_WRITE	0x20089	RDONLY	NONE
566	DENY_ALL	0x30196	WRONLY	NONE

Setting the maximum open files on a connection

Use the command line to set the maximum number of files that can be open concurrently.

Procedure

- Enter: `cifs option set maxopenfiles value`.

The *value* for the maximum number of files that can be open concurrently on a given connection is an integer from 128 to 59412. The default is 10000.

Note

The system has a maximum limit of 600 CIFS connections and 10,000 open files. However, if the system runs out of open files, the number of files can be increased.

Because each open file requires a certain amount of memory, the server may run out of memory if you set the value to the maximum. If a value is not within the accepted range, the system automatically resets it to 128 or 59412, depending on whether the value was below 128 or above 59412.

Data Domain system clock

When using active directory mode for CIFS access, the Data Domain System clock time can differ by no more than five minutes from that of the domain controller.

The DD System Manager, **System Settings** > **General Configuration** > **Time and Date Settings** option synchronizes the clock with a time server.

Because the Windows domain controller obtains the time from an external source, NTP must be configured. See the Microsoft documentation on how to configure NTP for the Windows operating system version or service pack that is running on your domain controller.

In active directory authentication mode, the Data Domain system periodically synchronizes the clock with a Windows Active Directory Domain Controller.

Synchronizing from a Windows domain controller

Use the command line on a Windows domain controller to synchronize with an NTP server.

Note

This example is for Windows 2003 SP1; substitute your domain server for the NTP server's name (*ntpservername*).

Procedure

1. On the Windows system, enter commands similar to the following:

```
C:\>w32tm /config /syncfromflags:manual /manualpeerlist: ntp-  
server-name C:\>w32tm /config /update C:\>w32tm /resync
```

2. After NTP is configured on the domain controller, configure the time server synchronization, as described in the section about working with time and date settings.

Synchronize from an NTP server

Configure the time server synchronization, as described in the section regarding working with time and date settings.

CHAPTER 9

NFS

This chapter includes:

- [NFS overview](#).....222
- [Managing NFS client access to the Data Domain system](#)..... 222
- [Displaying NFS information](#)..... 226
- [Integrating a DDR into a Kerberos domain](#)..... 228
- [Add and delete KDC servers after initial configuration](#)..... 229

NFS overview

Network File System (NFS) clients can have access to the system directories or MTrees on the Data Domain system.

- The `/backup` directory is the default destination for non-MTree compressed backup server data.
- The `/data/coll/backup` path is the root destination when using MTrees for compressed backup server data.
- The `/ddvar/core` directory contains Data Domain System core and log files (remove old logs and core files to free space in this area).

Note

You can also delete core files from the `/ddvar` or the `/ddvar/ext` directory if it exists.

Clients, such as backup servers that perform backup and restore operations with a Data Domain System, need access to the `/backup` or `/data/coll/backup` areas. Clients that have administrative access need to be able to access the `/ddvar/core` directory to retrieve core and log files.

As part of the initial Data Domain system configuration, NFS clients were configured to access these areas. This chapter describes how to modify these settings and how to manage data access.

Note

- For information about the initial system configuration, see the *EMC Data Domain Operating System Initial Configuration Guide*.
 - The `nfs` command manages backups and restores between NFS clients and Data Domain systems, and it displays NFS statistics and status. For complete information about the `nfs` command, see the *EMC Data Domain Operating System Command Reference Guide*.
 - For information about setting up third-party clients to use the Data Domain system as a server, see the related tuning guide, such as the *Solaris System Tuning*, which is available from the Data Domain support web site. From the Documentation > Integration Documentation page, select the vendor from the list and click **OK**. Select the tuning guide from the list.
-

Managing NFS client access to the Data Domain system

The topics in this section describe how to manage NFS client access to a Data Domain System.

Enabling NFS services

Enable NFS services to allow the client to access the system using the NFS protocol.

Procedure

1. Select the Data Domain system from the Navigation tree.
The Summary page for the system appears.
2. Select the **Data Management** › **NFS** tabs.
The NFS view showing the Exports tab appears.
3. Click **Enable**.

Disabling NFS services

Disable NFS services to prevent the client access to the system using the NFS protocol.

Procedure

1. Select the Data Domain system from the Navigation tree.
The Summary page for the system appears.
2. Select the **Data Management** › **NFS** tabs.
The NFS view showing the Exports tab appears.
3. Click **Disable**.

Creating an export

You can use Data Domain System Manager's Create button on the NFS view or use the Configuration Wizard to specify the NFS clients that can access the `/backup`, `/data/coll/backup`, `/ddvar`, `/ddvar/core` areas, or the `/ddvar/ext` area if it exists.

A Data Domain system supports a maximum number of 128 NFS exports.² And 900 simultaneous connections are allowed.

Note

You have to assign client access to each export separately and remove access from each export separately. For example, a client can be removed from `/ddvar` and still have access to `/data/coll/backup`.

CAUTION

If Replication is to be implemented, a single destination Data Domain system can receive backups from both CIFS clients and NFS clients as long as separate directories or MTrees are used for each. Do not mix CIFS and NFS data in the same area.

Procedure

1. Select the Data Domain system from the Navigation tree.
The Summary page for this system appears.

2. May be affected by hardware limitations.

2. Select the **Data Management** > **NFS** tabs.

The NFS view showing the Exports tab appears.

3. Click **Create**.

The Create NFS Exports dialog box appears.

4. Enter the pathname in the Directory Path text box (for example, `/data/col1/backup/dir1`).

Note

`col1` uses the lower-case letter L followed by the number 1.

5. In the Clients area, select an existing client or click the + icon to create a client.

The Client dialog box is displayed.

- a. Enter a server name in the text box.

Enter fully qualified domain names, hostnames, or IP addresses. A single asterisk (*) as a wild card indicates that all backup servers are to be used as clients.

Note

Clients given access to the `/data/col1/backup` directory have access to the entire directory. A client given access to a subdirectory of `/data/col1/backup` has access only to that subdirectory.

- A client can be a fully-qualified domain hostname, an IPv4 or IPv6 IP address, an IPv4 address with either a netmask or prefix length, an IPv6 address with prefix length, an NIS netgroup name with the prefix @, or an asterisk (*) wildcard with a domain name, such as `*.yourcompany.com`.
- A client added to a subdirectory under `/data/col1/backup` has access only to that subdirectory.
- Enter an asterisk (*) as the client list to give access to all clients on the network.

- b. Select the checkboxes of the NFS options for the client.

General:

- Read-only permission (ro).
- Allow connections from ports below 1024 (secure) (default).
- Log NFS request arguments (log). This option may impact performance.

Anonymous UID/GID:

- Map requests from UID (user identifier) or GID (group identifier) 0 to the anonymous UID/GID (root_squash).
- Map all user requests to the anonymous UID/GID (all_squash).
- Use Default Anonymous UID/GID.

Allowed Kerberos Authentication Modes:

- Unauthenticated connections (sec=sys). Select to not use authentication.
- Authenticated Connections (sec=krb5).

Note

Integrity and Privacy are not supported.

- c. Click **OK**.
6. Click **OK** to create the export.

Modifying an export

Change the directory path, domain name, and other options using the GUI.

Procedure

1. Select the Data Domain system from the Navigation tree.
The Summary page for this system appears.
2. Select the **Data Management** > **NFS** tabs.
The NFS view showing the Exports tab appears.
3. Click the checkbox of an export in the NFS Exports table.
4. Click **Modify**.
The Modify NFS Exports dialog box appears.
5. Modify the pathname in the Directory Path text box.
6. In the Clients area, select another client or click the + icon to create a client.
The Clients dialog box appears.
 - a. Enter a server name in the text box.
Enter fully qualified domain names, hostnames, or IP addresses. A single asterisk (*) as a wild card indicates that all backup servers are to be used as clients.

Note

Clients given access to the `/data/col1/backup` directory have access to the entire directory. A client given access to a subdirectory of `/data/col1/backup` has access only to that subdirectory.

- A client can be a fully-qualified domain hostname, an IPv4 or IPv6 IP address, an IPv4 address with either a netmask or prefix length, an IPv6 address with prefix length, an NIS netgroup name with the prefix @, or an asterisk (*) wildcard with a domain name, such as `*.yourcompany.com`.
A client added to a subdirectory under `/data/col1/backup` has access only to that subdirectory.
 - Enter an asterisk (*) as the client list to give access to all clients on the network.
- b. Select the checkboxes of the NFS options for the client.
General:

- Read-only permission (ro).
- Allow connections from ports below 1024 (secure) (default).
- Log NFS request arguments (log). This option may impact performance.

Anonymous UID/GID:

- Map requests from UID (user identifier) or GID (group identifier) 0 to the anonymous UID/GID (root_squash).
- Map all user requests to the anonymous UID/GID (all_squash).
- Use Default Anonymous UID/GID.

Allowed Kerberos Authentication Modes:

- Unauthenticated connections (sec=sys). Select to not use authentication.
- Authenticated Connections (sec=krb5).

Note

Integrity and Privacy are not supported.

- c. Click **OK**.
7. Click **OK** to modify the export.

Creating an export from an existing export

Create an export from an existing export and then modify it as needed.

Procedure

1. In the NFS Exports table, click the checkbox of the export you wish to use as the source.
2. Click **Create From**.
The Create NFS Export From dialog box appears.
3. Modify the export information, as described in section about modifying an export.

Deleting an export

Delete an export from the NFS Exports table.

Procedure

1. In the NFS Exports table, click the checkbox of the export you wish to delete.
2. Click **Delete**.
The Warning dialog box appears.
3. Click **OK** and **Close** to delete the export.

Displaying NFS information

The topics in this section describe how to use the DD System Manager to monitor NFS client status and NFS configuration.

Viewing NFS status

Display whether NFS is active and Kerberos is enabled.

Procedure

1. Log into the DD System Manager.
2. Select the Data Domain system in the Navigation tree.
3. Click the **Data Management** › **NFS** tabs.

The top panel shows the operational status of NFS; for example, whether NFS is currently active and running, and whether Kerberos mode is enabled.

Note

Click **Configure** to view the **System Settings** › **Access Management** › **Authentication** page where you can configure Kerberos authentication.

Viewing NFS exports

See the list of clients allowed to access the Data Domain System.

Procedure

1. Log into the DD System Manager.
2. Select the Data Domain system in the Navigation panel.
3. Select the **Data Management** › **NFS** tabs.

The Exports view shows a table of NFS exports that are configured for Data Domain System and the mount path, status, and NFS options for each export.

4. Click an export in the table to populate the Detailed Information area, below the Exports table.

In addition to the export's directory path, configured options, and status, the system displays a list of clients.

Use the Filter By text box to sort by mount path.

Click **Update** for the system to refresh the table and use the filters supplied.

Click **Reset** for the system to clear the Path and Client filters.

Viewing active NFS clients

Display all clients that have been connected in the past 15 minutes and their mount path.

Procedure

1. Log into the DD System Manager.
2. Select the Data Domain system in the Navigation panel.
3. Select the **Data Management** › **NFS** › **Active Clients** tabs.

The Active Clients view displays, showing all clients that have been connected in the past 15 minutes and their mount path.

Use the Filter By text boxes to sort by mount path and client name.

Click **Update** for the system to refresh the table and use the filters supplied.

Click **Reset** for the system to clear the Path and Client filters.

Integrating a DDR into a Kerberos domain

Set the domain name, the host name, and the DNS server for the DDR.

Enable the DDR to use the authentication server as a Key Distribution Center (for UNIX) and as a Distribution Center (for Windows Active Directory).

CAUTION

The examples provided in this description are specific to the operating system (OS) used to develop this exercise. You must use commands specific to your OS.

Note

For UNIX Kerberos mode, a keytab file must be transferred from the Key Distribution Center (KDC) server, where it is generated, to the DDR. If you are using more than one DDR, each DDR requires a separate keytab file. The keytab file contains a shared secret between the KDC server and the DDR.

Note

When using a UNIX KDC, the DNS server does not have to be the KDC server, it can be a separate server.

Procedure

1. Set the host name and the domain name for the DDR, using DDR commands.

```
net set hostname <host>
net set {domainname <local-domain-name>}
```

Note

The host name is the name of the DDR.

2. Configure NFS principal (node) for the DDR on the Key Distribution Center (KDC).

Example:

```
addprinc nfs/hostname@realm
```

Note

Hostname is the name for the DDR.

3. Verify that there are nfs entries added as principals on the KDC.

Example:

```
listprincs
nfs/hostname@realm
```

4. Add the DDR principal into a keytab file.

Example:

```
ktadd <keytab_file> nfs/hostname@realm
```

- Verify that there is an nfs keytab file configured on the KDC.

Example:

```
klist -k <keytab_file>
```

Note

The <keytab_file> is the keytab file used to configure keys in a previous step.

- Copy the keytab file from the location where the keys for NFS DDR are generated to the DDR in the /ddvar/ directory.

Table 102 Keytab destination

Copy file from:	Copy file to:
<keytab_file> (The keytab file configured in a previous step.)	/ddvar/

- Set the realm on the DDR, using the following DDR command:

```
authentication kerberos set realm <home realm> kdc-type <unix, windows.> kdc <IP address of server>
```

- When the kdc-type is UNIX, import the keytab file from /ddvar/ to /ddr/etc/, where the Kerberos configuration file expects it. Use the following DDR command to copy the file:

```
authentication kerberos keytab import
```

NOTICE

This step is required only when the kdc-type is UNIX.

Kerberos setup is now complete.

- To add a NFS mount point to use Kerberos, use the nfs add command.

See the *EMC Data Domain Operating System Command Reference Guide* for more information.

- Add host, NFS and relevant user principals for each NFS client on the Key Distribution Center (KDC).

Example: **listprincs**

```
host/hostname@realm
nfs/hostname@realm
root/hostname@realm
```

- For each NFS client, import all its principals into a keytab file on the client.

Example:

```
ktadd -k <keytab_file> host/hostname@realm
```

```
ktadd -k <keytab_file> nfs/hostname@realm
```

Add and delete KDC servers after initial configuration

After you have integrated a DDR into a Kerberos domain, and thereby enabled the DDR to use the authentication server as a Key Distribution Center (for UNIX) and as a Distribution

Center (for Windows Active Directory), you can use the following procedure to add or delete KDC servers.

Procedure

1. Join the DDR to a Windows Active Directory (AD) server or a UNIX Key Distribution Center (KDC).

```
authentication kerberos set realm <home-realm> kdc-type {windows
[kdcs <kdc-list>] | unix kdcs <kdc-list>}
```

Example: `authentication kerberos set realm krb5.test kdc-type unix kdcs nfskrb-kdc.krb5.test`

This command joins the system to the `krb5.test` realm and enables Kerberos authentication for NFS clients.

Note

A keytab generated on this KDC must exist on the DDR to authenticate using Kerberos.

2. Verify the Kerberos authentication configuration.

```
authentication kerberos show config
Home Realm:          krb5.test
KDC List:            nfskrb-kdc.krb5.test
KDC Type:           unix
```

3. Add a second KDC server.

```
authentication kerberos set realm <home-realm> kdc-type {windows
[kdcs <kdc-list>] | unix kdcs <kdc-list>}
```

Example: `authentication kerberos set realm krb5.test kdc-type unix kdcs ostqa-sparc2.krb5.test nfskrb-kdc.krb5.test`

Note

A keytab generated on this KDC must exist on the DDR to authenticate using Kerberos.

4. Verify that two KDC servers are added.

```
authentication kerberos show config
Home Realm:          krb5.test
KDC List:            ostqa-sparc2.krb5.test, nfskrb-kdc.krb5.test
KDC Type:           unix
```

5. Display the value for the Kerberos configuration key.

```
reg show config.keberos
config.kerberos.home_realm = krb5.test
config.kerberos.home_realm.kdc1 = ostqa-sparc2.krb5.test
config.kerberos.home_realm.kdc2 = nfskrb-kdc.krb5.test
config.kerberos.kdc_count = 2
config.kerberos.kdc_type = unix
```

6. Delete a KDC server.

Delete a KDC server by using the `authentication kerberos set realm <home-realm> kdc-type {windows [kdcs <kdc-list>] | unix kdcs <kdc-list>}` command without listing the KDC server that you want to delete. For example, if the existing KDC servers are `kdc1`, `kdc2`, and `kdc3`, and you want to remove `kdc2` from the realm, you could use the following example:

```
authentication kerberos set realm <realm-name> kdc-type <kdc_type>  
kdcserver kdc1,kdc3
```


CHAPTER 10

SCSI Target

This chapter includes:

- [SCSI Target overview](#) 234
- [Working with physical resources](#) 235
- [Fibre Channel view](#) 242
- [Working with access groups](#) 243
- [Working with a selected access group](#) 245
- [Adding an access group device](#) 245
- [Modifying or deleting an access group device](#) 247
- [Configuring the NDMP device TapeServer group](#) 248
- [Differences in FC link monitoring among DD OS versions](#) 250

SCSI Target overview

SCSI (Small Computer System Interface) Target is a unified management daemon for all SCSI services and transports. SCSI Target supports both VTL (Virtual Tape Library) and DD Boost over FC (Fibre Channel) and supports anything that has a target LUN (logical unit number) on a DD system.

SCSI Target Services and Transports

The SCSI Target daemon starts when FC ports are present or VTL is licensed. It provides unified management for all SCSI Target *services* and *transports*.

- A *service* is anything that has a target LUN on a DD system that uses SCSI Target commands, such as VTL (tape drives and changers), DD Boost over FC (processor devices), or vDisk (Virtual Disk Device).
- A *transport* enables *devices* to become visible to *initiators*.
 - An *initiator* is a backup client that connects to a system to read and write data using the FC protocol. A specific initiator can support DD Boost over FC or VTL, but not both.
 - *Devices* are visible on a SAN (storage area network) through physical ports. Host initiators communicate with the DD system through the SAN.
 - *Access groups* manage access between devices and initiators.
 - An *endpoint* is the logical target on a DD system to which the initiator connects. You can disable, enable, and rename endpoints. To be able to delete endpoints, the associated transport hardware must no longer exist. Endpoints are automatically discovered and created when a new transport connection occurs. Endpoints have the following attributes: port topology, FCP2-RETRY status, WWPN, and WWNN.

Note the following:

- VTL and DD Boost over FC can run on the same system, but they cannot share the same HBA (host bus adapter) ports.
- DD Boost can service both FC and IP clients simultaneously; however, both transports cannot share the same initiator.
- Only one initiator should be present per access group. Each access group is assigned a type (VTL or DD Boost over FC).

SCSI Target Architectures - Supported and Unsupported

SCSI Target supports the following architectures:

- **VTL plus DD Boost over FC from different initiators:** Two different initiators (on the same or different clients) may access a DD system using VTL and DD Boost over FC, through the same or different DD system target endpoints.
- **VTL plus DD Boost over FC from one initiator to two different DD systems:** A single initiator may access two different DD systems using any service.

SCSI Target does not support the following architecture:

- **VTL plus DD Boost over FC from one initiator to the same DD system:** A single initiator may not access the same DD system through different services.

For More Information about DD Boost and the `sscscitarget` Command (CLI)

For more information about using DD Boost through the DD System Manager, see the related chapter in this book. For other types of information about DD Boost, see the *EMC Data Domain Boost for OpenStorage Administration Guide*.

This chapter focuses on using SCSI Target through the DD System Manager. After you have become familiar with basic tasks, the `scsitaraget` command in the *EMC Data Domain Operating System Command Reference Guide* provides more advanced management tasks.

When there is heavy VTL traffic, avoid running the `scsitaraget group use` command, which switches the in-use endpoint lists for one or more SCSI Target or vdisk devices in a group between primary and secondary endpoint lists.

Working with physical resources

Selecting **Physical Resources** > **Physical Resources** displays information about initiators and endpoints. An *initiator* is a backup client that connects to a system to read and write data using the Fibre Channel (FC) protocol. A specific initiator can support DD Boost over FC or VTL, but not both. An *endpoint* is the logical target on a DD system to which the initiator connects.

Table 103 Initiators tab

Item	Description
Name	Name of initiator, which is either the WWPN or the alias assigned to the initiator.
WWPN	Unique worldwide port name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the Fibre Channel (FC) port.
WWNN	Unique worldwide node name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the FC node.
Online Endpoints	Group name where ports are seen by initiator. Displays <i>None</i> or <i>Offline</i> if the initiator is unavailable.

Table 104 Endpoints tab

Item	Description
Name	Specific name of endpoint.
WWPN	Unique worldwide port name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the Fibre Channel (FC) port.
WWNN	Unique worldwide node name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the FC node.
Physical Port	Physical port number.
Enabled	HBA (host bus adapter) port operational state, which is either <i>Yes</i> (enabled) or <i>No</i> (not enabled).
Status	DD system VTL link status, which is either <i>Online</i> (capable of handling traffic) or <i>Offline</i> .

Configure Resources

Selecting **Configure Resources** takes you to the Fibre Channel area for Physical Resources, where you can configure endpoints and initiators.

Working with initiators

Selecting **Physical Resources > Physical Resources > Initiators** displays information about initiators. An *initiator* is a client system FC HBA (fibre channel host bus adapter) WWPN (worldwide port name) with which the DD system interfaces. An *initiator name* is an alias for the client's WWPN, for ease of use.

While a client is mapped as an initiator – but before an access group has been added – the client cannot access any data on a DD system.

After adding an access group for the initiator or client, the client can access only the devices in that access group. A client can have access groups for multiple devices.

An access group may contain multiple initiators, but an initiator can exist in only one access group.

Note

A maximum of 1024 initiators can be configured for a DD system.

Table 105 Initiator information

Item	Description
Name	Name of initiator.
Group	Group associated with initiator.
Online Endpoints	Endpoints seen by initiator. Displays <i>none</i> or <i>offline</i> if initiator is unavailable.
WWPN	Unique worldwide port name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the Fibre Channel (FC) port.
WWNN	Unique worldwide node name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the FC node.
Vendor Name	Name of vendor for initiator.

Selecting **Configure Initiators** takes you to the Fibre Channel area for Physical Resources.

CLI Equivalent

```
# vtl initiator show
Initiator  Group      Status  WWNN              WWPN              Port
-----
tsm6_p1   tsm3500_a  Online  20:00:00:24:ff:31:ce:f8  21:00:00:24:ff:31:ce:f8  10b

Initiator  Symbolic Port Name              Address Method
-----
tsm6_p1   QLE2562 FW:v5.06.03 DVR:v8.03.07.15.05.09-k  auto
```

Adding or configuring an initiator

Add initiators to provide backup clients to connect to the system to read and write data using the FC (Fibre Channel) protocol. A specific initiator can support DD Boost over FC, or VTL, but not both. A maximum of 1024 initiators can be configured for a DD system.

Procedure

1. Select **Configure Initiators**, which takes you to **Hardware > Fibre Channel > Physical Resources**.
2. Under Initiators, select Add (+) to display the Add Initiator dialog.
3. Enter the port's unique WWPN in the specified format.
4. Enter a Name for the initiator.
5. Select the Address Method: **Auto** is used for standard addressing, and **VSA** (Volume Set Addressing) is used primarily for addressing virtual buses, targets, and LUNs.
6. Select **OK**.

CLI Equivalent

```
# scsitarget group add My_Group initiator My_Initiator
```

Modifying or deleting an initiator

Before you can delete an initiator, it must be offline and not attached to any group. Otherwise, you will get an error message, and the initiator will not be deleted. You must delete all initiators in an access group before you can delete the access group.

Procedure

1. Select **Configure Initiators**, which takes you to **Hardware > Fibre Channel > Physical Resources**.
2. Under Initiators, select one of the initiators. If you want to delete it, select the delete (X) icon. If you want to modify it, select the edit (pencil) icon to display the Modify Initiator dialog.
3. You can change the initiator's Name and Address Method [**Auto** is used for standard addressing, and **VSA** (Volume Set Addressing) is used primarily for addressing virtual buses, targets, and LUNs.]
4. Select **OK**.

Recommendation to Set Initiator Aliases - CLI only

It is strongly recommended that Initiator aliases be set to reduce confusion and human error during the configuration process.

```
# vtl initiator set alias NewAliasName wwpn 21:00:00:e0:8b:9d:0b:e8
# vtl initiator show
Initiator  Group  Status  WWNN  WWPN  Port
-----  -
NewVTL    aussie1  Online  20:00:00:e0:8b:9d:0b:e8  21:00:00:e0:8b:9d:0b:e8  6a
          Offline  20:00:00:e0:8b:9d:0b:e8  21:00:00:e0:8b:9d:0b:e8  6b

Initiator  Symbolic Port Name  Address Method
-----  -
NewVTL    -----  auto
-----  -----  -----
```

Working with endpoints

Selecting **Physical Resources** > **Physical Resources** > **Endpoints** provides information about endpoint hardware and connectivity. To change an endpoint's name, FCP2 Retry enablement, and/or topology, select **Configuring Endpoints**.

Table 106 Hardware Tab

Item	Description
Name	Specific name of endpoint.
Model	Model of hardware.
Firmware	DD system HBA (host bus adapter) firmware version.
WWPN	Unique worldwide port name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the Fibre Channel (FC) port.
WWNN	Unique worldwide node name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the FC node.
Physical Port	Physical port number.

Table 107 Endpoints Tab

Item	Description
Endpoint	Specific name of endpoint.
Connection Type	Connection type, such as N-Port, loop, or SAN (storage area network).
Link Speed	Transmission speed of link, in Gbps (Gigabits per second).
Port ID	Port identifier.
Enabled	HBA (host bus adapter) port operational state, which is either <i>Yes</i> (enabled) or <i>No</i> (not enabled).
Status	DD system VTL link status, which is either <i>Online</i> (capable of handling traffic) or <i>Offline</i> .

Configure Endpoints

Selecting **Configure Endpoints** takes you to the Fibre Channel area for Physical Resources, where you can change the name, FCP2 Retry enablement, and/or topology.

CLI Equivalent

```
# scsitarget endpoint show list
Endpoint      System Address  Transport      Enabled  Status
-----
endpoint-fc-0 5a              FibreChannel  Yes      Online
endpoint-fc-1 5b              FibreChannel  Yes      Online
```

Working with a selected endpoint

Selecting **Physical Resources** > **Physical Resources** > **Endpoints** > *endpoint* provides information about the endpoint's hardware, connectivity, and statistics.

Table 108 Hardware tab

Item	Description
Name	Specific name of endpoint.
Model	Model of hardware.
Firmware	DD system HBA (host bus adapter) firmware version.
WWPN	Unique worldwide port name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the Fibre Channel port.
WWNN	Unique worldwide node name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the FC node.
Physical Port	Physical port number.

Table 109 Summary tab

Item	Description
Endpoint	Specific name of endpoint.
Connection Type	Connection type, such as N-Port, loop, or SAN (storage area network).
Link Speed	Transmission speed of link, in Gbps (Gigabits per second).
Port ID	Port identifier.
Enabled	HBA (host bus adapter) port operational state, which is either <i>Yes</i> (enabled) or <i>No</i> (not enabled).
Status	DD system VTL link status, which is either <i>Online</i> (capable of handling traffic) or <i>Offline</i> .

Table 110 Statistics tab

Item	Description
Endpoint	Specific name of endpoint.
Library	Name of library containing the endpoint.
Device	Number of device.
Ops/s	Operations per second.
Read KiB/s	Speed of reads in KiB per second.
Write KiB/s	Speed of writes in KiB per second.

Table 111 Detailed Statistics tab

Item	Description
Endpoint	Specific name of endpoint.
# of Control Commands	Number of control commands.
# of Read Commands	Number of read commands.
# of Write Commands	Number of write commands.
In (MiB)	Number of MiB written (the binary equivalent of MB).
Out (MiB)	Number of MiB read.
# of Error Protocol	Number of error protocols.
# of Link Fail	Number of link failures.
# of Invalid Crc	Number of invalid CRCs (cyclic redundancy checks).
# of Invalid TxWord	Number of invalid tx (transmission) words.
# of Lip	Number of LIPs (loop initialization primitives).
# of Loss Signal	Number of signals or connections that have been lost.
# of Loss Sync	Number of signals or connections that have lost synchronization.

Selecting endpoints for a device

Since endpoints connect a device to an initiator, use this process to set up the endpoints before you connect the device.

Procedure

1. Select **Access Groups** > **Groups** > *group*.
2. Select **More Tasks** > **Endpoints** > **Set In-Use**.
3. In the Set in-Use Endpoints dialog, select only specific devices, or select **Devices** to select all devices in the list.
4. Indicate whether the endpoints are primary or secondary.
5. Select **OK**.

Adding or configuring an endpoint

Add endpoints to provide a logical target on a DD system to which an initiator connects.

Procedure

1. Select **Hardware** > **Fibre Channel** > **Physical Resources**.
2. Under **Endpoints**, select an endpoint, and then select **Configure**.
3. In the Configure Endpoint dialog, enter a name for the endpoint (1 to 28 characters). The field cannot be empty or be the word “all,” and cannot contain the characters asterisk (*), question mark (?), front or back slashes (/, \), or right or left parentheses [(,)].
4. Uncheck **Enabled** next to **FCP2 Retry**, if you do *not* want the endpoint to support retransmission of data during data recovery.
5. Select one of these options for the topology.

- **Default**, which is loop preferred
- **Loop Only**
- **Point to Point**
- **Loop Preferred**

6. Select **OK**.

Enabling an endpoint

Endpoints must be enabled before they can be connected to an initiator.

Procedure

1. Select **Hardware** › **Fibre Channel** › **Physical Resources**.
2. Select **More Tasks** › **Endpoints** › **Enable**. If all endpoints are already enabled, a message to that effect is displayed.
3. In the Enable Endpoints dialog, select one or more endpoints from the list, and select **Next**.
4. After the confirmation, select **Next** to complete the task.

Disabling an endpoint

Before disabling an endpoint, make sure that it is not in use.

Procedure

1. Select **Hardware** › **Fibre Channel** › **Physical Resources**.
2. Select **More Tasks** › **Endpoints** › **Disable**.
3. In the Disable Endpoints dialog, select one or more endpoints from the list, and select **Next**. If an endpoint is in use, you are warned that deleting it might disrupt the system.
4. Select **Next** to complete the task.

Modifying an endpoint's system address

You can modify the active system address for a SCSI Target endpoint using the `scsitararget endpoint modify` command option. This is useful if the endpoint is associated with a system address that no longer exists, for example after a controller upgrade or when a controller HBA (host bus adapter) has been moved. When the system address for an endpoint is modified, all properties of the endpoint, including WWPN and WWNN (worldwide port and node names, respectively), if any, are preserved and are used with the new system address.

In the following example, endpoint ep-1 was assigned to system address 5a, but this system address is no longer valid. A new controller HBA was added at system address 10a. The SCSI Target subsystem automatically created a new endpoint, ep-new, for the newly discovered system address. Because only a single endpoint can be associated with a given system address, ep-new must be deleted, and then ep-1 must be assigned to system address 10a.

Note

It may take some time for the modified endpoint to come online, depending on the SAN environment, since the WWPN and WWNN have moved to a different system address. You may also need to update SAN zoning to reflect the new configuration.

Procedure

1. Show all endpoints to verify the endpoints to be changed:

```
# scsitarget endpoint show list
```

2. Disable all endpoints:

```
# scsitarget endpoint disable all
```

3. Delete the new, unnecessary endpoint, ep-new:

```
# scsitarget endpoint del ep-new
```

4. Modify the endpoint you want to use, ep-1, by assigning it the new system address 10a:

```
# scsitarget endpoint modify ep-1 system-address 10a
```

5. Enable all endpoints:

```
# scsitarget endpoint enable all
```

Setting a hard address (loop ID)

Some backup software requires that all private-loop targets have a hard address (loop ID) that does not conflict with another node. The range for a loop ID is from 0 to 125.

Procedure

1. Select **Hardware > Fibre Channel > Physical Resources**.
2. Select **More Tasks > Set Loop ID**.
3. In the Set Loop ID dialog, enter the loop ID (from 0 to 125), and select **OK**.

Fibre Channel view

The Fibre Channel view displays two tabs: Physical Resources and Access Groups. Physical resources include initiators and endpoints. An access group holds a collection of initiator WWPNs (worldwide port names) or aliases and the drives and changers they are allowed to access.

Physical Resources view

The **Hardware > Fibre Channel > Physical Resources** tab displays information about endpoints and initiators. Select a single endpoint to view additional information in the Endpoint Details area.

Table 112 Endpoints

Item	Description
Name	Name of endpoint.
WWPN	Unique worldwide port name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the Fibre Channel (FC) port.
WWNN	Unique worldwide node name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the FC node
Physical Port	Physical port number.

Table 112 Endpoints (continued)

Item	Description
Enabled	Port operational state; either Enabled or Disabled.
Link Status	Either Online or Offline; that is, whether or not the port is up and capable of handling traffic.

Table 113 Initiators

Item	Description
Name	Name of initiator.
Service	Service support by the initiator, which is either VTL, DD Boost, or vDisk.
WWPN	Unique worldwide port name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the Fibre Channel (FC) port.
WWNN	Unique worldwide node name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the FC node.
Vendor Name	Initiator's model.
Online Endpoints	Endpoints seen by this initiator. Displays <code>none</code> or <code>offline</code> if the initiator is not available.

Access Groups view

The Access Group tab lists access groups by group name, service (VTL, DD Boost, or vDisk), endpoints, initiators, and number of devices. Selecting a link to Configure DD Boost groups or VTL groups takes you to the DD Boost or VTL page, where you can create an access group.

Working with access groups

Access groups hold a collection of initiator WWPNs (worldwide port names) or aliases and the drives and changers they are allowed to access. A VTL default group named *TapeServer* lets you add devices that will support NDMP (Network Data Management Protocol)-based backup applications.

Access group configuration allows initiators (in general backup applications) to read and write data to devices in the same access group.

Access groups let clients access only selected LUNs (media changers or virtual tape drives) on a system. A client set up for an access group can access only devices in its access group.

Avoid making access group changes on a DD system during active backup or restore jobs. A change may cause an active job to fail. The impact of changes during active jobs depends on a combination of backup software and host configurations.

Selecting **Data Management** > **VTL** > **Access Groups** > **Groups** displays the following information for all access groups.

Table 114 Access group information

Item	Description
Group Name	Name of group.
Initiators	Number of initiators in group.
Devices	Number of devices in group.

If you select **View All Access Groups**, you are taken to the Fibre Channel view. From the More Tasks menu, you can create or delete a group.

Creating an access group

Access groups manage access between devices and initiators. Do not use the default TapeServer access group unless you are using NDMP.

Procedure

1. Select **Data Management** > **VTL** > **Access Groups** > **Groups**.
2. Select **More Tasks** > **Group** > **Create**
3. In the Create Access Group dialog, enter a name, from 1 to 128 characters, and select **Next**.
4. Add devices, and select **Next**.
5. Review the summary, and select **Finish** or **Back**, as appropriate.

CLI Equivalent

```
# scsitaraget group create My_Group service My_Service
```

Deleting an access group

Before you can delete an access group, you must remove all of its initiators and LUNs.

Procedure

1. Remove all of the initiators and LUNs from the group.
2. Select **Data Management** > **VTL** > **Access Groups** > **Groups**.
3. Select **More Tasks** > **Group** > **Delete**.
4. In the Delete Group dialog, select the checkbox of the group to be removed, and select **Next**.
5. In the groups confirmation dialog, verify the deletion, and select **Submit**.
6. Select **Close** when the Delete Groups Status displays **Completed**.

CLI Equivalent

```
# scsitaraget group destroy My_Group
```

Working with a selected access group

Selecting **Data Management** > **VTL** > **Access Groups** > **Groups** > *group* displays the following information for a selected access group.

Table 115 LUNs tab

Item	Description
LUN	Device address – maximum number is 16383. A LUN can be used only once within a group, but can be used again within another group. VTL devices added to a group must use contiguous LUNs.
Library	Name of library associated with LUN.
Device	Changers and drives.
In-Use Endpoints	Set of endpoints currently being used: primary or secondary.
Primary Endpoints	Initial (or default) endpoint used by backup application. In the event of a failure on this endpoint, the secondary endpoints may be used, if available.
Secondary Endpoints	Set of fail-over endpoints to use if primary endpoint fails.

Table 116 Initiators tab

Item	Description
Name	Name of initiator, which is either the WWPN or the alias assigned to the initiator.
WWPN	Unique worldwide port name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the Fibre Channel port.

From the More Tasks menu, with a group selected, you can configure that group, or set endpoints in use.

Adding an access group device

Access group configuration allows initiators (in general backup applications) to read and write data to devices in the same access group.

Procedure

1. Select **Data Management** > **VTL** > **Access Groups** > **Groups**. You can also select a specific *group*.
2. Select **More Tasks** > **Group** > **Create** or **Group** > **Configure**.
3. In the Create or Modify Access Group dialog, enter or modify the **Group Name** if desired. (This field is required.)
4. To configure initiators to the access group, check the box next to the initiator. You can add initiators to the group later.

5. Select **Next**.

6. In the Devices display, select Add (+) to display the Add Devices dialog.
 - a. Verify that the correct library is selected in the Library Name drop-down list, or select another library.
 - b. In the Device area, select the checkboxes of the devices (changer and drives) to be included in the group.
 - c. Optionally, specify a starting LUN in the LUN Start Address text box.

This is the LUN that the DD system returns to the initiator. Each device is uniquely identified by the library and the device name. (For example, it is possible to have drive 1 in Library 1 and drive 1 in Library 2). Therefore, a LUN is associated with a device, which is identified by its library and device name.

When presenting LUNs via attached FC ports on VTL cards, ports can be designated as primary, secondary, or none. A Primary port for a set of LUNs is the port that is currently advertizing those LUNs to a fabric. A secondary port is a port that will broadcast a set of LUNs in the event of primary path failure (this requires manual intervention). A setting of none is used in the case where you do not wish to advertize selected LUNs. The presentation of LUNs depends on the SAN topology in question.

The initiators in the access group interact with the LUN devices that are added to the group.

The maximum LUN accepted when creating an access group is 16383.

A LUN can be used only once for an individual group. The same LUN can be used with multiple groups.

Some VTL initiators (clients) have specific rules for VTL target LUN numbering; for example, requiring LUN 0 or requiring contiguous LUNs. If these rules are not followed, an initiator may not be able to access some or all of the LUNs assigned to a VTL target port.

Check your initiator documentation for special rules, and if necessary, alter the device LUNs on the VTL target port to follow the rules. For example, if an initiator requires LUN 0 to be assigned on the VTL target port, check the LUNs for devices assigned to ports, and if there is no device assigned to LUN 0, change the LUN of a device so it is assigned to LUN 0.

- d. In the Primary and Secondary Endpoints area, select an option to determine from which ports the selected device will be seen. The following conditions apply for designated ports:
 - all – The checked device is seen from all ports.
 - none – The checked device is not seen from any port.
 - select – The checked device is to be seen from selected ports. Select the checkboxes of the appropriate ports.
 - If only primary ports are selected, the checked device is visible only from primary ports.
 - If only secondary ports are selected, the checked device is visible only from secondary ports. Secondary ports can be used if the primary ports become unavailable.

The switchover to a secondary port is not an automatic operation. You must manually switch the VTL device to the secondary ports if the primary ports become unavailable.

The port list is a list of physical port numbers. A port number denotes the PCI slot and a letter denotes the port on a PCI card. Examples are 1a, 1b, or 2a, 2b.

A drive appears with the same LUN on all the ports that you have configured.

- e. Select **OK**.

You are returned to the Devices dialog box where the new group is listed. To add more devices, repeat these five substeps.

7. Select **Next**.

8. Select **Close** when the `Completed` status message is displayed.

CLI Equivalent

```
# vtl group add VTL_Group vtl NewVTL changer lun 0 primary-port all secondary-port all
# vtl group add VTL_Group vtl NewVTL drive 1 lun 1 primary-port all secondary-port all
# vtl group add Setup_Test vtl Setup_Test drive 3 lun 3 primary-port endpoint-fc-0
secondary-port endpoint-fc-1
```

```
# vtl group show Setup_Test
```

```
Group: Setup_Test
```

```
Initiators:
```

Initiator Alias	Initiator WWPN
tsm6_p23	21:00:00:24:ff:31:ce:f8

```
Devices:
```

Device Name	LUN	Primary Ports	Secondary Ports	In-use Ports
Setup_Test changer	0	all	all	all
Setup_Test drive 1	1	all	all	all
Setup_Test drive 2	2	5a	5b	5a
Setup_Test drive 3	3	endpoint-fc-0	endpoint-fc-1	endpoint-fc-0

Modifying or deleting an access group device

You may need to modify or delete a device from an access group.

Procedure

1. Select **Data Management** › **VTL** › **Access Groups** › **Groups** › *group*.
2. Select **More Tasks** › **Group** › **Configure**.
3. In the Modify Access Group dialog, enter or modify the **Group Name**. (This field is required.)
4. To configure initiators to the access group, check the box next to the initiator. You can add initiators to the group later.
5. Select **Next**.
6. Select a device, and select the edit (pencil) icon to display the Modify Devices dialog. Then, follow steps a-e. If you simply want to delete the device, select the delete (X) icon, and skip to step e.
 - a. Verify that the correct library is selected in the Library drop-down list, or select another library.
 - b. In the Devices to Modify area, select the checkboxes of the devices (Changer and drives) to be modified.

- c. Optionally, modify the starting LUN (logical unit number) in the LUN Start Address box.

This is the LUN that the DD system returns to the initiator. Each device is uniquely identified by the library and the device name. (For example, it is possible to have drive 1 in Library 1 and drive 1 in Library 2). Therefore, a LUN is associated with a device, which is identified by its library and device name.

The initiators in the access group interact with the LUN devices that are added to the group.

The maximum LUN accepted when creating an access group is 16383.

A LUN can be used only once for an individual group. The same LUN can be used with multiple groups.

Some VTL initiators (clients) have specific rules for VTL target LUN numbering; for example, requiring LUN 0 or requiring contiguous LUNs. If these rules are not followed, an initiator may not be able to access some or all of the LUNs assigned to a VTL target port.

Check your initiator documentation for special rules, and if necessary, alter the device LUNs on the VTL target port to follow the rules. For example, if an initiator requires LUN 0 to be assigned on the VTL target port, check the LUNs for devices assigned to ports, and if there is no device assigned to LUN 0, change the LUN of a device so it is assigned to LUN 0.

- d. In the Primary and Secondary Ports area, change the option that determines the ports from which the selected device is seen. The following conditions apply for designated ports:
- all – The checked device is seen from all ports.
 - none – The checked device is not seen from any port.
 - select – The checked device is seen from selected ports. Select the checkboxes of the ports from which it will be seen.
If only primary ports are selected, the checked device is visible only from primary ports.
If only secondary ports are selected, the checked device is visible only from secondary ports. Secondary ports can be used if primary ports become unavailable.
- The switchover to a secondary port is not an automatic operation. You must manually switch the VTL device to the secondary ports if the primary ports become unavailable.
- The port list is a list of physical port numbers. A port number denotes the PCI slot, and a letter denotes the port on a PCI card. Examples are 1a, 1b, or 2a, 2b.
- A drive appears with the same LUN on all ports that you have configured.
- e. Select **OK**.

Configuring the NDMP device TapeServer group

The VTL TapeServer group holds tape drives that interface with NDMP (Network Data Management Protocol)-based backup applications and that send control information and data streams over IP (Internet Protocol) instead of Fibre Channel (FC). A device used by the NDMP TapeServer must be in the VTL group TapeServer and is available *only* to the NDMP TapeServer.

Procedure

1. Add tape drives to a new or existing library (in this example, named “dd660-16”).
2. Create slots and CAPs for the library.
3. Add the created devices in a library (in this example, “dd660-16”) to the TapeServer access group.
4. Enable the NDMP daemon by entering at the command line:

```
# ndmpd enable
Starting NDMP daemon, please wait.....
NDMP daemon is enabled.
```

5. Ensure that the NDMP daemon sees the devices in the TapeServer group:

```
# ndmpd show devicenames
NDMP Device      Virtual Name      Vendor   Product          Serial Number
-----
/dev/dd_ch_c0t010 dd660-16 changer  STK      L180             6290820000
/dev/dd_st_c0t110 dd660-16 drive 1  IBM      ULTRIUM-TD3     6290820001
/dev/dd_st_c0t210 dd660-16 drive 2  IBM      ULTRIUM-TD3     6290820002
/dev/dd_st_c0t310 dd660-16 drive 3  IBM      ULTRIUM-TD3     6290820003
/dev/dd_st_c0t410 dd660-16 drive 4  IBM      ULTRIUM-TD3     6290820004
-----
```

6. Add an NDMP user (ndmp in this example) with the following command:

```
# ndmpd user add ndmp
Enter password:
Verify password:
```

7. Verify that user ndmp is added correctly:

```
# ndmpd user show
ndmp
```

8. Display the NDMP configuration:

```
# ndmpd option show all
Name              Value
-----
authentication    text
debug             disabled
port              10000
preferred-ip      -----
```

9. Change the default user password authentication to use MD5 encryption for enhanced security, and verify the change (notice the authentication value changed from text to md5):

```
# ndmpd option set authentication md5
# ndmpd option show all
Name              Value
-----
authentication    md5
debug             disabled
port              10000
preferred-ip      -----
```

Results

NDMP is now configured, and the TapeServer access group shows the device configuration. See the `ndmpd` chapter of the *EMC Data Domain Operating System Command Reference Guide* for the complete command set and options.

Differences in FC link monitoring among DD OS versions

Different releases of DD OS handle FC (Fibre Channel) Link Monitoring in different ways.

DD OS 5.3 and later

Port monitoring detects an FC port at system startup and raises an alert if the port is enabled and offline. To clear the alert, disable an unused port using the `scsitarget` or `vtl` commands.

DD OS 5.1 up to 5.3

If a port is offline, an alert notifies you that the link is down. This alert is managed, which means it stays active until cleared. This occurs when the VTL FC port is online or disabled. If the port is not in use, disable it unless it needs to be monitored.

DD OS 5.0 up to 5.1

If a port is offline, an alert notifies you that the link is down. The alert is not managed, which means it does not stay active and does not appear in the current alerts list. When the port is online, an alert notifies you that the link is up. If the port is not in use, disable it unless it needs to be monitored.

DD OS 4.9 up to 5.0

An FC port must be included in a VTL group to be monitored.

CHAPTER 11

Working with DD Boost

This chapter includes:

- [About Data Domain Boost software](#)..... 252
- [Managing DD Boost with DD System Manager](#)..... 252
- [About interface groups](#)..... 265
- [Destroying DD Boost](#)..... 270
- [Configuring DD Boost-over-Fibre Channel](#)..... 271
- [About the DD Boost tabs](#)..... 275

About Data Domain Boost software

Data Domain Boost (DD Boost) software provides advanced integration with backup and enterprise applications for increased performance and ease of use. DD Boost distributes parts of the deduplication process to the backup server or application clients, enabling client-side deduplication for faster, more efficient backup and recovery.

DD Boost software is an optional product that requires a separate license to operate on the Data Domain system. You can purchase a DD Boost software license key for a Data Domain system directly from EMC Data Domain.

There are two components to DD Boost: one component that runs on the backup server and another that runs on the Data Domain system.

- In the context of the EMC NetWorker backup application, EMC Avamar backup application and other DDBoost partner backup applications, the component that runs on the backup server (DD Boost libraries) is integrated into the particular backup application.
- In the context of Symantec backup applications (NetBackup and Backup Exec) and the Oracle RMAN plug-in, you need to download an appropriate version of the DD Boost plugin that is installed on each media server. The DD Boost plugin includes the DD Boost libraries for integrating with the DD Boost server running on the Data Domain system.

A Data Domain system can be a single Data Domain system or a gateway.

The backup application (for example, Avamar, NetWorker, NetBackup, or Backup Exec) sets policies that control when backups and duplications occur. Administrators manage backup, duplication, and restores from a single console and can use all of the features of DD Boost, including WAN-efficient replicator software. The application manages all files (collections of data) in the catalog, even those created by the Data Domain system.

In the Data Domain system, storage units that you create are exposed to backup applications that use the DD Boost protocol. For Symantec applications, storage units are viewed as disk pools. For NetWorker, storage units are viewed as logical storage units (LSUs). A storage unit is an MTree; therefore, it supports MTree quota settings. (Do not create an MTree in place of a storage unit.)

This chapter does not contain installation instructions; refer to the documentation for the product you want to install. For example, for information about setting up DD Boost with Symantec backup applications (NetBackup and Backup Exec), see the *EMC Data Domain Boost for OpenStorage Administration Guide*. For information on setting up DD Boost with any other application, see the application-specific documentation.

Additional information about configuring and managing DD Boost on the Data Domain system can also be found in the *EMC Data Domain Boost for OpenStorage Administration Guide*.

Managing DD Boost with DD System Manager

Access the DD Boost view in System Manager.

Procedure

1. Select the Data Domain system in the Navigation panel.
2. Verify that the file system is enabled and running by selecting **Data Management** › **File System** and checking the state.

3. Select **Data Management** > **DD Boost** to access the DD Boost view.

If you go to the DD Boost page without a license, the Status states that DD Boost is not licensed. Click Add License and enter a valid license in the Add License Key dialog box.

Use the DD Boost tabs—Settings, Active Connections, IP Network, Fibre Channel, and Storage Units—to manage DD Boost.

Specifying DD Boost user names

A DD Boost user is also a DD OS user. Specify a DD Boost user either by selecting an existing DD OS user name or by creating a new DD OS user name and making that name a DD Boost user.

Backup applications use the DD Boost user name and password to connect to the Data Domain system. You must configure these credentials on each backup server that connects to this system. The Data Domain system supports multiple DD Boost users. For complete information about setting up DD Boost with Symantec NetBackup and Backup Exec, see the *EMC Data Domain Boost for OpenStorage Administration Guide*. For information on setting up DD Boost with any other application, see the application-specific documentation.

Procedure

1. Select **Data Management** > **DD Boost** > **Settings**.

2. Select **Add (+)** above the DD Boost user list.

The Add User dialog appears.

3. To select an existing user, select the user name in the drop-down list.

EMC recommends that you select a username with management role privileges set to *none*.

4. To create and select a new user, select **Create a new Local User** and do the following:

- a. Enter the new user name in the User dialog.

The user must be configured in the backup application to connect to the Data Domain system.

- b. Enter the password twice in the appropriate dialogs.

5. Select **OK**.

Changing DD Boost user passwords

Change a DD Boost user password.

Procedure

1. Select **Data Management** > **DD Boost** > **Settings**.

2. Select a user in the DD Boost user list.

3. Click the **Edit** button (pencil icon) above the DD Boost user list.

The Change Password dialog appears.

4. Enter the password twice in the appropriate boxes.

5. Click **Change**.

Removing a DD Boost user name

Remove a user from the DD Boost access list.

Procedure

1. Select **Data Management > DD Boost > Settings**.
2. Select the user in the DD Boost user list that needs to be removed.
3. Click **Remove (X)** above the DD Boost user list.

The Remove User dialog appears.

4. Click **Remove**.

After removal, the user remains in the DD OS access list.

Enabling DD Boost

Use the DD Boost Settings tab to enable DD Boost and to select or add a DD Boost user.

Procedure

1. In the DD Boost Settings tab, click **Enable** in the DD Boost Status area.
The Enable DD Boost dialog box is displayed.
2. Select an existing user name from the menu, or add a new user by supplying the name, password, and role.

Disabling DD Boost

Disabling DD Boost drops all active connections to the backup server. When you disable or destroy DD Boost, the DD Boost FC service is also disabled.

Before you begin

Ensure there are no jobs running from your backup application before disabling.

Note

File replication started by DD Boost between two Data Domain restores is not canceled.

Procedure

1. In the DD Boost Settings tab, click **Disable** in the DD Boost Status area.
2. Click **OK** in the Disable DD Boost confirmation dialog box.

Viewing DD Boost storage units

Access the Storage Units tab to view and manage DD Boost storage units.

The DD Boost Storage Unit tab:

- Lists the storage units and provides the following information for each storage unit:

Table 117 Storage unit information

Item	Description
Storage Unit	The name of the storage unit.

Table 117 Storage unit information (continued)

Item	Description
Quota Hard Limit	The percentage of hard limit quota used.
Last 24 hr Pre-Comp	The amount of raw data from the backup application that has been written in the last 24 hours.
Last 24 hr Post-Comp	The amount of storage used after compression in the last 24 hours.
Last 24 hr Comp Ratio	The compression ratio for the last 24 hours.
Weekly Avg Post-Comp	The average amount of compressed storage used in the last five weeks.
Last Week Post-Comp	The average amount of compressed storage used in the last seven days.
Weekly Avg Comp Ratio	The average compression ratio for the last five weeks.
Last Week Comp Ratio	The average compression ratio for the last seven days.

- Allows you to create a new storage unit and to delete an existing one selected from the list.
- Displays four related tabs for a storage unit selected from the list: Storage Unit, Space Usage, Daily Written, and Data Movement.
- Takes you to the Replication > DD Boost > File Replication tab when you click the **View DD Boost Replications** link.

Note

A DD Replicator license is required for DD Boost to display tabs other than the File Replication tab.

Creating a storage unit

You must create at least one storage unit on the Data Domain system, and a DD Boost user must be assigned to that storage unit. Use the Storage Units tab to create a storage unit.

Each storage unit is a top-level subdirectory of the `/data/coll` directory; there is no hierarchy among storage units.

Procedure

1. Go to **Data Management > DD Boost > Storage Units**.
2. Click the **Create (+)** button.

The Create Storage Unit dialog box is displayed.

3. Enter the storage unit name in the Name box.

Each storage unit name must be unique. Storage unit names can be up to 50 characters. The following characters are acceptable:

- upper- and lower-case alphabetical characters: A-Z, a-z
- numbers: 0-9

- embedded space
 - comma (,)
 - period (.), as long as it does not precede the name
 - exclamation mark (!)
 - number sign (#)
 - dollar sign (\$)
 - per cent sign (%)
 - plus sign (+)
 - at sign (@)
 - equal sign (=)
 - ampersand (&)
 - semi-colon (;)
 - parenthesis [(and)]
 - square brackets ([and])
 - curly brackets ({and})
 - caret (^)
 - tilde (~)
 - apostrophe (unslanted single quotation mark)
 - single slanted quotation mark (')
 - minus sign (-)
 - underscore (_)
4. To select an existing username that will have access to this storage unit, select the user name in the dropdown list.
- EMC recommends that you select a username with management role privileges set to *none*.
5. To create and select a new username that will have access to this storage unit, select **Create a new Local User** and:
- a. Enter the new user name in the User box.
The user must be configured in the backup application to connect to the Data Domain system.
 - b. Enter the password twice in the appropriate boxes.
6. To set storage space restrictions to prevent a storage unit from consuming excess space: enter either a soft or hard limit quota setting, or both a hard and soft limit. With a soft limit an alert is sent when the storage unit size exceeds the limit, but data can still be written to it. Data cannot be written to the storage unit when the hard limit is reached.

Note

Quota limits are pre-compressed values. To set quota limits, select **Set to Specific Value** and enter the value. Select the unit of measurement: MiB, GiB, TiB, or PiB.

Note

When setting both soft and hard limits, a quota's soft limit cannot exceed the quota's hard limit.

7. Click **Create**.
8. Repeat the above steps for each Data Domain Boost-enabled system.

Viewing storage unit information

From the DD Boost Storage Units tab, you can select a storage unit and access the Storage Unit, Space Usage, Daily Written, and Data Movement tabs for the selected storage unit.

Storage Unit tab

The Storage Unit tab shows detailed information for a selected storage unit in its Summary and Quota panels. The Snapshot panel shows snapshot details, allows you to create new snapshots and schedules, and provides a link to the **Data Management > Snapshots** tab.

- The Summary panel shows summarized information for the selected storage unit.

Table 118 Summary panel

Summary item	Description
Total Files	The total number of file images on the storage unit. For compression details that you can download to a log file, click the Download Compression Details link. The generation can take up to several minutes. After it has completed, click Download.
Full Path	/data/col1/filename
Tenant Unit	Lists the tenant unit if one is assigned to the selected storage unit.
Status	R: read; W: write; Q: quota defined
Pre-Comp Used	The amount of pre-compressed storage already used.

- The Quota panel shows quota information for the selected storage unit.

Table 119 Quota panel

Quota item	Description
Quota Enforcement	Enabled or disable. Clicking Quota takes you to the Data Management > Quota tab where you can configure quotas.
Pre-Comp Soft Limit	Current value of soft quota set for the storage unit.
Pre-Comp Hard Limit	Current value of hard quota set for the storage unit.
Quota Summary	Percentage of Hard Limit used.

To modify the pre-comp soft and hard limits shown in the tab:

1. Click the **Configure** button in the Quota panel.
2. In the Configure Quota dialog box, enter values for hard and soft quotas and select the unit of measurement: MiB, GiB, TiB, or PiB. Click **OK**.

- **Snapshot**
The Snapshot panel shows information about the storage unit's snapshots.

Table 120 Snapshot panel

Item	Description
Total Snapshots	The total number of snapshots created for this MTree. A total of 750 snapshots can be created for each MTree.
Expired	The number of snapshots in this MTree that have been marked for deletion, but have not been removed with the clean operation as yet.
Unexpired	The number of snapshots in this MTree that are marked for keeping.
Oldest Snapshot	The date of the oldest snapshot for this MTree.
Newest Snapshot	The date of the newest snapshot for this MTree.
Next Scheduled	The date of the next scheduled snapshot.
Assigned Snapshot Schedules	The name of the snapshot schedule assigned to this MTree.

- Do one of the following:
 - Assign a snapshot schedule to a selected storage unit: Click **Assign Snapshot Schedules**. Select the schedule's checkbox; click **OK** and **Close**.
 - Create a new schedule: Click **Assign Snapshot Schedules**. Enter the new schedule's name.

Note

Snapshot name pattern can be composed only of letters, numbers, `_`, `-`, `%d`, `%a`, `%m`, `%b`, `%y`, `%Y`, `%H`, and `%M`, following the pattern shown in the dialog box. Enter the new pattern and click **Validate Pattern & Update Sample**. Click **Next**.

- Select when the schedule is to be executed: weekly, every day (or selected days), monthly on specific days that you select by clicking that date in the calendar, or on the last day of the month. Click **Next**.
- Enter the times of the day when the schedule is to be executed: Either select **At Specific Times** or **In Intervals**. If you select a specific time, select the time from the list. Click **Add (+)** to add a time (24-hour format). For intervals, select **In Intervals** and set the start and end times and how often (**Every**), such as every eight hours. Click **Next**.
- Enter the retention period for the snapshots in days, months, or years. Click **Next**.
- Review the Summary of your configuration. Click **Back** to edit any of the values. Click **Finish** to create the schedule.

- Clicking the Snapshots link takes you to the **Data Management > Snapshots** tab.

Space Usage tab

The Space Usage tab graph displays a visual representation of data usage for the storage unit over time.

- Click a point on a graph line to display a box with data at that point.
- Click **Print** (at the bottom on the graph) to open the standard Print dialog box.
- Click **Show in new window** to display the graph in a new browser window.

There is one type of graph data displayed: Post-comp Used.

Post-comp Used—The total amount of disk storage in use on the storage unit. Shown with the Space Used (left) vertical axis of the graph.

Daily Written tab

The Daily Written view contains a graph that displays a visual representation of data that is written daily to the system over a period of time, selectable from 7 to 120 days. The data amounts are shown over time for pre- and post-compression amounts.

Data Movement tab

A graph in the same format as the Daily Written graph that shows the amount of disk space moved to the Extended Retention storage area (if the Archive license is enabled).

Modifying a storage unit

Use the Modify Storage Unit dialog to rename a storage unit, select a different existing user, create and select a new user, and edit quota settings.

Procedure

1. Go to **Data Management > DD Boost > Storage Units**.
2. In the Storage Unit list, select the storage unit to modify.
3. Click the pencil icon.

The Modify Storage Unit dialog appears.

4. To rename the storage unit, edit the text in the **Name** field.
5. To select a different existing user, select the user name in the drop-down list.

EMC recommends that you select a username with management role privileges set to *none*.

6. To create and select a new user, select **Create a new Local User** and do the following:
 - a. Enter the new user name in the User box.

The user must be configured in the backup application to connect to the Data Domain system.

- b. Enter the password twice in the appropriate boxes.
7. Edit the Quota Settings as needed.

To set storage space restrictions to prevent a storage unit from consuming excess space: enter either a soft or hard limit quota setting, or both a hard and soft limit. With a soft limit an alert is sent when the storage unit size exceeds the limit, but data can still be written to it. Data cannot be written to the storage unit when the hard limit is reached.

Note

Quota limits are pre-compressed values. To set quota limits, select **Set to Specific Value** and enter the value. Select the unit of measurement: MiB, GiB, TiB, or PiB.

Note

When setting both soft and hard limits, a quota's soft limit cannot exceed the quota's hard limit.

8. Click **Modify**.

Renaming a storage unit

Use the Modify Storage Unit dialog to rename a storage unit.

Renaming a storage unit changes the name of the storage unit while retaining its:

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

Procedure

1. Go to **Data Management > DD Boost > Storage Units**.
2. In the Storage Unit list, select the storage unit to rename.
3. Click the pencil icon.
The Modify Storage Unit dialog appears.
4. Edit the text in the **Name** field.
5. Click **Modify**.

Deleting a storage unit

Use the Storage Units tab to delete a storage unit from your Data Domain system. Deleting a storage unit removes the storage unit, as well as any images contained in the storage unit, from your Data Domain system.

Procedure

1. Go to **Data Management > DD Boost > Storage Units**.
2. Select the storage unit to be deleted from the list.
3. Click **Delete (X)**.
4. Click **OK**.

Results

The storage unit is removed from your Data Domain system. You must also manually remove the corresponding backup application catalog entries.

Undeleting a storage unit

Use the Storage Units tab to undelete a storage unit.

Undeleting a storage unit recovers a previously 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.

Procedure

1. Go to **Data Management** › **DD Boost** › **Storage Units**.
2. From the **More Tasks** menu, select **Undelete Storage Unit...**
3. In the Undelete Storage Units dialog box, select the storage unit(s) that you want to undelete.
4. Click **OK**.

Selecting DD Boost options

Use the Set DD Boost Options dialog to specify settings for distributed segment processing, virtual synthetics, low bandwidth optimization for file replication, file replication encryption, and file replication network preference (IPv4 or IPv6).

Procedure

1. To display the DD Boost option settings, go to **Data Management** › **DD Boost** › **Settings** and expand the Advanced Options list.
2. To change the settings, select **Set Options** in the **More Tasks** menu.
The Set DD Boost Options dialog appears.
3. Select any option to be enabled.
4. Deselect any option to be disabled.
To deselect a File Replication Network Preference option, select the other option.
5. Click **OK**.

Note

You can manage distributed segment processing via the `ddbboost option` commands, which are described in detail in the *EMC Data Domain Operating System Command Reference Guide*.

Distributed segment processing

Distributed segment processing increases backup throughput in almost all cases by eliminating duplicate data transmission between the media server and the Data Domain system.

You can manage distributed segment processing via the `ddbboost option` commands, which are described in detail in the *EMC Data Domain Operating System Command Reference Guide*.

Note

Distributed segment processing is enabled by default with EMC Data Domain Extended Retention (formerly Data Domain Archiver) configurations and cannot be disabled.

Virtual synthetics

A virtual synthetic full backup is the combination of the last full (synthetic or full) backup and all subsequent incremental backups. Virtual synthetics are enabled by default.

Low-bandwidth optimization

If you use file replication over a low-bandwidth network (WAN), you can increase replication speed by using low bandwidth optimization. This feature provides additional compression during data transfer. Low bandwidth compression is available to Data Domain systems with an installed Replication license.

Low-bandwidth optimization, which is disabled by default, is designed for use on networks with less than 6 Mbps aggregate bandwidth. Do not use this option if maximum file system write performance is required.

Note

You can also manage low bandwidth optimization via the `ddboost file-replication` commands, which are described in detail in the *EMC Data Domain Operating System Command Reference Guide*.

File replication encryption

You can encrypt the data replication stream by enabling the DD Boost file replication encryption option.

Note

If DD Boost file replication encryption is used on systems without the Data at Rest option, it must be set to on for both the source and destination systems.

Managed file replication TCP port setting

For DD Boost managed file replication, use the same global listen port on both the source and target Data Domain systems. To set the listen port, use the `replication option` command as described in the *EMC Data Domain Operating System Command Reference Guide*.

File replication network preference

Use this option to set the preferred network type for DD Boost file replication to either IPv4 or IPv6.

Managing certificates for DD Boost

A host certificate allows DD Boost client programs to verify the identity of the system when establishing a connection. CA certificates identify certificate authorities that should be trusted by the system. The topics in this section describe how to manage host and CA certificates for DD Boost.

Adding a host certificate for DD Boost

Add a host certificate to your system. DD OS supports one host certificate for DD Boost.

Procedure

1. If you have not yet requested a host certificate, request one from a trusted CA.

2. When you have received a host certificate, copy or move it to the computer from which you run DD Service Manager.
3. Start DD System Manager on the system to which you want to add a host certificate.

Note

DD System Manager supports certificate management only on the management system (which is the system running DD System Manager).

4. Expand **DD Network** in the Navigation panel and select the management system.
5. Select **Data Management > DD Boost**.
6. Select **More Tasks > Manage Certificates**.

Note

If you try to remotely manage certificates on a managed system, DD System Manager displays an information message at the top of the certificate management dialog. To manage certificates for a system, you must start DD System Manager on that system.

7. In the Host Certificate area, click **Add**.
8. To add a host certificate enclosed in a .p12 file, do the following:
 - a. Select **I want to upload the certificate as a .p12 file**.
 - b. Type the password in the **Password** box.
 - c. Click **Browse** and select the host certificate file to upload to the system.
 - d. Click **Add**.
9. To add a host certificate enclosed in a .pem file, do the following:
 - a. Select **I want to upload the public key as a .pem file and use a generated private key**.
 - b. Click **Browse** and select the host certificate file to upload to the system.
 - c. Click **Add**.

Adding CA certificates for DD Boost

Add a certificate for a trusted CA to your system. DD OS supports multiple certificates for trusted CAs.

Procedure

1. Obtain a certificate for the trusted CA.
2. Copy or move the trusted CA certificate to the computer from which you run DD Service Manager.
3. Start DD System Manager on the system to which you want to add the CA certificate.

Note

DD System Manager supports certificate management only on the management system (which is the system running DD System Manager).

4. Expand **DD Network** in the Navigation panel and select the management system.
5. Select **Data Management > DD Boost**.

6. Select **More Tasks** > **Manage Certificates**.

Note

If you try to remotely manage certificates on a managed system, DD System Manager displays an information message at the top of the certificate management dialog. To manage certificates for a system, you must start DD System Manager on that system.

7. In the CA Certificates area, click **Add**.

The Add CA Certificate for DD Boost dialog appears.

8. To add a CA certificate enclosed in a .pem file, do the following:

- a. Select **I want to upload the certificate as a .pem file**.
- b. Click **Browse**, select the host certificate file to upload to the system, and click **Open**.
- c. Click **Add**.

9. To add a CA certificate using copy and paste, do the following:

- a. Copy the certificate text to the clipboard using the controls in your operating system.
- b. Select **I want to copy and paste the certificate text**.
- c. Paste the certificate text in the box below the copy and paste selection.
- d. Click **Add**.

Managing DD Boost client access and encryption

Use the DD Boost Settings tab to configure which specific clients, or set of clients, can establish a DD Boost connection with the Data Domain System and whether or not the client will use encryption. By default, the system is configured to allow all clients to have access, with no encryption.

Note

Enabling in-flight encryption will impact system performance.

Adding a DD Boost client

Create an allowed DD Boost client and specify whether the client will use encryption.

Procedure

1. Select **Data Management** > **DD Boost** > **Settings**.
2. In the Allowed Clients section, click **Create (+)**.

The Add Allowed Client dialog appears.

3. Enter the hostname of the client.

This can be a fully-qualified domain name (e.g. host1.emc.com) or a hostname with a wildcard (e.g. *.emc.com).

4. Select the Encryption Strength.

The options are None (no encryption), Medium (AES128-SHA1), or High (AES256-SHA1).

5. Select the Authentication Mode.
The options are One Way, Two Way, or Anonymous.
6. Click **OK**.

Modifying a DD Boost client

Change the name, encryption strength, and authentication mode of an allowed DD Boost client.

Procedure

1. Select **Data Management** > **DD Boost** > **Settings**.
2. In the Allowed Clients list, select the client to modify.
3. Click the **Edit** button, which displays a pencil icon.
The Modify Allowed Client dialog appears.
4. To change the name of a client, edit the Client text.
5. To change the Encryption Strength, select the option.
The options are None (no encryption), Medium (AES128-SHA1), or High (AES256-SHA1).
6. To change the Authentication Mode, select the option.
The options are One Way, Two Way, or Anonymous.
7. Click **OK**.

Removing a DD Boost client

Delete an allowed DD Boost client.

Procedure

1. Select **Data Management** > **DD Boost** > **Settings**.
2. Select the client from the list.
3. Click the **Delete (X)** button, which displays a pencil icon.
The Delete Allowed Clients dialog appears.
4. Confirm and select the client name. Click **OK**.

About interface groups

This feature lets you combine multiple Ethernet links into a group and register only one interface on the Data Domain system with the backup application. The DD Boost Library negotiates with the Data Domain system to obtain the best interface to send data. Load balancing provides higher physical throughput to the Data Domain system.

Configuring an interface group creates a private network within the Data Domain system, comprised of the IP addresses designated as a group. Clients are assigned to a single group, and the group interface uses load balancing to improve data transfer performance and increase reliability.

For example, in the Symantec NetBackup environment, media server clients use a single public network IP address to access the Data Domain system. All communication with the Data Domain system is initiated via this administered IP connection, which is configured on the NetBackup server.

If an interface group is configured, when the Data Domain system receives data from the media server clients, the data transfer is load-balanced and distributed on all the interfaces in the group, providing higher input/output throughput, especially for customers who use multiple 1 GigE connections.

The data transfer is load-balanced based on the number of connections outstanding on the interfaces. Only connections for backup and restore jobs are load-balanced. Check the Active Connections for more information on the number of outstanding connections on the interfaces in a group.

Should an interface in the group fail, all the in-flight jobs to that interface are automatically resumed on healthy operational links (unknown to the backup applications). Any jobs that are started subsequent to the failure are also routed to a healthy interface in the group. If the group is disabled or an attempt to recover on an alternate interface fails, the administered IP is used for recovery. Failure in one group will not utilize interfaces from another group.

Consider the following information when managing interface groups.

- The IP address must be configured on the Data Domain system, and its interface enabled. To check the interface configuration, see the Network Settings tab in the **Hardware > Network** page, and check for free ports. See the `net` chapter of the *EMC Data Domain Operating System Command Reference Guide* or the *EMC Data Domain Operating System Initial Configuration Guide* for information about configuring an IP address for an interface.
- You can use the `ddbboost ifgroup` commands to manage interface groups; these commands are described in detail in the *EMC Data Domain Operating System Command Reference Guide*.
- Interface groups provide full 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. For details, see the *EMC Data Domain Boost Administration Guide*.
- Configured interfaces are listed in Active Connections, on the lower portion of the Activities page.

The topics that follow describe how to manage interface groups.

Interfaces

IFGROUP supports physical and virtual interfaces.

An IFGROUP interface is a member of a single IFGROUP `<group-name>` and may consist of:

- Physical interface such as `eth0a`
- Virtual interface, created for link failover or link aggregation, such as `veth1`
- Virtual alias interface such as `eth0a:2` or `veth1:2`
- Virtual VLAN interface such as `eth0a.1` or `veth1.1`
- Within an IFGROUP `<group-name>`, all interfaces must be on unique interfaces (Ethernet, virtual Ethernet) to ensure failover in the event of network error.

IFGROUP provides full 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.

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

Clients

IFGROUP supports various naming formats for clients. Client selection is based on a specified order of precedence.

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 for the client, such as `ddboost`
- Client public IP range, such as `128.5.20.0/24`

Prior to write or read processing, the client requests an IFGROUP IP address from the server. To select the client IFGROUP association, the client information is evaluated according to the following order of precedence.

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. If there is already an active connection between the client and the Data Domain system, and the connection exists on the interface in the IFGROUP, then the IFGROUP interfaces are made available for the client.
5. Connected client IP range. An IP mask check is done against the client source IP; if the client's source IP address matches the mask in the IFGROUP clients list, then the IFGROUP interfaces are made available for the client.
 - For IPv4, `xx.xx.xx.0/24` provides a 24-bit mask against the connecting IP. The /24 represents what bits are masked when the client's source IP address is evaluated for access to the IFGROUP.
 - For IPv6, `xxxx::0/112` provides a 112-bit mask against the connecting IP. The /112 represents what bits are masked when the client's source IP address is evaluated for access to the IFGROUP.

This host-range check is useful for separate VLANs with many clients where there isn't a unique partial hostname (domain).

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

Interface enforcement

IFGROUP lets you 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*.

Creating interface groups

Use the IP Network tab to create interface groups and to add interfaces and clients to the groups.

Multiple interface groups improve the efficiency of DD Boost by allowing you to:

- Configure DD Boost to use specific interfaces configured into groups.
- Assign clients to one of those interface groups.
- Monitor which interfaces are active with DD Boost clients.

Create interface groups first, and then add clients (as new media servers become available) to an interface group.

Procedure

1. On the IP Network tab, select the Add (+) button associated with interface groups.
2. Enter the interface group name.
3. Select one or more interfaces. A maximum of 32 interfaces can be configured.

Note

Depending upon aliasing configurations, some interfaces may not be selectable if they are sharing a physical interface with another interface in the same group. This is because each interface within the group must be on a different physical interface to ensure fail-over recovery.

4. Click **OK**.
5. Select Add (+) associated with clients.
6. Enter a fully qualified client name or `*.mydomain.com`.

Note

The * client is initially available to the default group. The * client may only be a member of one ifgroup.

7. Select a previously configured interface group, and click **OK**.

Deleting an interface group

Use the IP Network tab to delete an interface group. Deleting an interface group deletes all interfaces and clients associated with the group.

Procedure

1. On the IP Network tab, select the interface group in the list. The default group cannot be deleted.
2. Click the associated Delete (X) button.
3. Confirm the deletion.

Enabling and disabling interface groups

Use the IP Network tab to enable and disable interface groups.

Procedure

1. On the IP Network tab, select the interface group in the list.

Note

If the interface group does not have both clients and interfaces assigned, you cannot enable the group.

2. Click the associated **Edit** (pencil) button.
3. Select the **Enabled** button to enable; deselect to disable.
4. Click **OK**.

Modifying an interface group's name and interfaces

Use the IP Network tab to change an interface group's name and the interfaces associated with the group.

Procedure

1. On the IP Network tab, select the interface group in the list.
2. Click the associated **Edit** (pencil) button.
3. Retype the name to modify the name.

The group name must be one to 24 characters long and contain only letters, numbers, underscores, and dashes. It cannot be the same as any other group name and cannot be "default", "yes", "no", or "all."

4. Select or deselect client interfaces in the Interfaces list.

Note

If you remove all interfaces from the group, it will be automatically disabled.

5. Click **OK**.

Deleting a client from the interface group

Use the IP Network tab to delete a client from an interface group.

Procedure

1. On the IP Network tab, select the client in the list.
2. Click the associated Delete (X) button.

Note

If the interface group to which it belongs has no other clients, the interface group is disabled.

3. Confirm the deletion.

Modifying a client's name or interface group

Use the IP Network tab to change a client's name or interface group.

Procedure

1. On the IP Network tab, select the client in the list.
2. Click the associated **Edit** (pencil) button.
3. Type a new client name.

Client names must be unique and may consist of:

- **FQDN**
- ***.domain**
- ***** (for the default group only)
- Client public IP range:
 - For IPv4, `xx.xx.xx.0/24` provides a 24-bit mask against the connecting IP. The /24 represents what bits are masked when the client's source IP address is evaluated for access to the IFGROUP.
 - For IPv6, `xxxx::0/112` provides a 112-bit mask against the connecting IP. The /112 represents what bits are masked when the client's source IP address is evaluated for access to the IFGROUP.

Client names have a maximum length of 128 characters.

4. Select a new interface group from the menu.

Note

The old interface group is disabled if it has no clients.

5. Click **OK**.

Destroying DD Boost

Use this option to permanently remove all of the data (images) contained in the storage units. When you disable or destroy DD Boost, the DD Boost FC service is also disabled. Only an administrative user can destroy DD Boost.

Procedure

1. Manually remove (expire) the corresponding backup application catalog entries.

Note

If multiple backup applications are using the same Data Domain system, then remove all entries from each of those applications' catalogs.

2. From the More Tasks menu, select **Destroy DD Boost**.
3. Enter your administrative credentials when prompted.
4. Click **OK**.

Configuring DD Boost-over-Fibre Channel

In earlier versions of DD OS, all communication between the DD Boost Library and any Data Domain system was performed using IP networking. DD OS now offers Fibre Channel as an alternative transport mechanism for communication between the DD Boost Library and the Data Domain system.

Note

Windows, Linux, HP-UX (64-bit Itanium architecture), and AIX client environments are supported.

Enabling DD Boost users

Before you can configure the DD Boost-over-FC service on a Data Domain system, you must add one or more DD Boost users and enable DD Boost.

Before you begin

- Log in to System Manager. For instructions, see “Logging In and Out of DD System Manager.”

CLI equivalent

```
login as: sysadmin
Data Domain OS 5.5.x.x-12345
Using keyboard-interactive authentication.
Password:
```

- If you are using the CLI, ensure that the SCSI target daemon is enabled:

```
# scsitaraget enable
Please wait ...
SCSI Target subsystem is enabled.
```

Note

If you are using System Manager, the SCSI target daemon is automatically enabled when you enable the DD Boost-over-FC service (later in this procedure).

- Verify that the DD Boost license is installed. In System Manager, select **Data Management** > **DD Boost** to access the DD Boost Settings tab. If the Status indicates that DD Boost is not licensed, click **Add License** and enter a valid license in the Add License Key dialog box.

CLI equivalents

```
# license show

# license add license-code
```

Procedure

1. Go to the **Data Management** > **DD Boost** > **Settings** tab.
2. On the **Settings** tab, specify one or more DD Boost user names.

A DD Boost user is also a DD OS user. When specifying a DD Boost user name, you can select an existing DD OS user name, or you can create a new DD OS user name and make that name a DD Boost user. This release supports multiple DD Boost users. For detailed instructions, see “Specifying DD Boost User Names.”

CLI equivalents

```
# user add username [password password]
```

```
# ddbboost set user-name exampleuser
```

- Click the **Enable Status** button to enable DD Boost.

CLI equivalent

```
# ddbboost enable
Starting DDBOOST, please wait.....
DDBOOST is enabled.
```

Results

You are now ready to configure the DD Boost-over-FC service on the Data Domain system.

Configuring DD Boost

After you have added user(s) and enabled DD Boost, you need to enable the Fibre Channel option and specify the DD Boost Fibre Channel server name. Depending on your application, you may also need to create one or more storage units and install the DD Boost API/plugin on media servers that will access the Data Domain system.

Procedure

- Go to the **Data Management > DD Boost > Fibre Channel** tab.
- Click the **Enable Status** button to enable Fibre Channel transport.

CLI equivalent

```
# ddbboost option set fc enabled
Please wait...
DD Boost option "FC" set to enabled.
```

- To change the DD Boost Fibre Channel server name from the default (hostname), click **Edit**, enter a new server name, and click **OK**.

CLI equivalent

```
# ddbboost fc dfc-server-name set DFC-ddbeta2
DDBoost dfc-server-name is set to "DFC-ddbeta2" for DDBoost FC.
Configure clients to use "DFC-DFC-ddbeta2" for DDBoost FC.
```

- Go to the **Data Management > DD Boost > Storage Units** tab to create a storage unit (if not already created by the application).

You must create at least one storage unit on the Data Domain system, and a DD Boost user must be assigned to that storage unit. For detailed instructions, see “Creating a Storage Unit.”

CLI equivalent

```
# ddbboost storage-unit create storage_unit_name-su
```

- Install the DD Boost API/plugin (if necessary, based on the application).

The DD Boost OpenStorage plug-in software must be installed on NetBackup media servers that need to access the Data Domain system. This plug-in includes the required DD Boost Library that integrates with the Data Domain system. For detailed installation and configuration instructions, see the *Data Domain Boost for OpenStorage Administration Guide* or the *Data Domain Boost Administration Guide*.

Results

You are now ready to verify connectivity and create access groups.

Verifying connectivity and creating access groups

Go to **Hardware > Fibre Channel > Physical Resources** to manage initiators and endpoints for access points. Go to **Data Management > DD Boost > Fibre Channel** to create and manage DD Boost-over-FC access groups.

Note

Avoid making access group changes on a Data Domain system during active backup or restore jobs. A change may cause an active job to fail. The impact of changes during active jobs depends on a combination of backup software and host configurations.

Procedure

1. Go to **Hardware > Fibre Channel > Physical Resources** to verify that initiators are present.

It is recommended that you assign aliases to initiators to reduce confusion during the configuration process.

CLI equivalent

```
# scsitarget initiator show list
Initiator      System Address      Group      Service
-----
initiator-1    21:00:00:24:ff:31:b7:16    n/a        n/a
initiator-2    21:00:00:24:ff:31:b8:32    n/a        n/a
initiator-3    25:00:00:21:88:00:73:ee    n/a        n/a
initiator-4    50:06:01:6d:3c:e0:68:14    n/a        n/a
initiator-5    50:06:01:6a:46:e0:55:9a    n/a        n/a
initiator-6    21:00:00:24:ff:31:b7:17    n/a        n/a
initiator-7    21:00:00:24:ff:31:b8:33    n/a        n/a
initiator-8    25:10:00:21:88:00:73:ee    n/a        n/a
initiator-9    50:06:01:6c:3c:e0:68:14    n/a        n/a
initiator-10   50:06:01:6b:46:e0:55:9a    n/a        n/a
tsm6_p23       21:00:00:24:ff:31:ce:f8    SetUp_Test VTL
-----
```

2. To assign an alias to an initiator, select one of the initiators and click the pencil (edit) icon. In the Name field of the Modify Initiator dialog, enter the alias and click **OK**.

CLI equivalents

```
# scsitarget initiator rename initiator-1 initiator-renamed
Initiator 'initiator-1' successfully renamed.
```

```
# scsitarget initiator show list
Initiator      System Address      Group      Service
-----
initiator-2    21:00:00:24:ff:31:b8:32    n/a        n/a
initiator-renamed  21:00:00:24:ff:31:b7:16    n/a        n/a
-----
```

3. On the Physical Resources tab, verify that endpoints are present and enabled.

CLI equivalent

```
# scsitarget endpoint show list
Endpoint      System Address      FibreChannel  Yes  Online
-----
endpoint-fc-0  5a                  FibreChannel  Yes  Online
endpoint-fc-1  5b                  FibreChannel  Yes  Online
-----
```

4. Go to **Data Management > DD Boost > Fibre Channel**.
5. In the DD Boost Access Groups area, click the **+** icon to add an access group.
6. Enter a unique name for the access group. Duplicate names are not supported.

CLI equivalent

```
# ddbboost fc group create test-dfc-group
DDBBoost FC Group "test-dfc-group" successfully created.
```

7. Select one or more initiators. Optionally, replace the initiator name by entering a new one. Click **Next**.

CLI equivalent

```
#ddbboost fc group add test-dfc-group initiator initiator-5
Initiator(s) "initiator-5" added to group "test-dfc-group".
```

An initiator is a port on an HBA attached to a backup client that connects to the system for the purpose of reading and writing data using the Fibre Channel protocol. The WWPN is the unique World-Wide Port Name of the Fibre Channel port in the media server.

8. Specify the number of DD Boost devices to be used by the group. This number determines which devices the initiator can discover and, therefore, the number of I/O paths to the Data Domain system. The default is one, the minimum is one, and the maximum is 64.

CLI equivalent

```
# ddbboost fc group modify Test device-set count 5
Added 3 devices.
```

See the *Data Domain Boost for OpenStorage Administration Guide* for the recommended value for different clients.

9. Indicate which endpoints to include in the group: all, none, or select from the list of endpoints. Click **Next**.

CLI equivalents

```
# scsitarget group add Test device ddbboost-dev8 primary-endpoint
all
secondary-endpoint all
Device 'ddbboost-dev8' successfully added to group.
```

```
# scsitarget group add Test device ddbboost-dev8 primary-endpoint
endpoint-fc-1 secondary-endpoint fc-port-0
Device 'ddbboost-dev8' is already in group 'Test'.
```

When presenting LUNs via attached FC ports on HBAs, ports can be designated as primary, secondary or none. A primary port for a set of LUNs is the port that is currently advertizing those LUNs to a fabric. A secondary port is a port that will broadcast a set of LUNs in the event of primary path failure (this requires manual intervention). A setting of none is used in the case where you do not wish to advertize selected LUNs. The presentation of LUNs is dependent upon the SAN topology.

10. Review the Summary and make any modifications. Click **Finish** to create the access group, which is displayed in the DD Boost Access Groups list.

CLI equivalent

```
# scsitarget group show detailed
```

Note

To change settings for an existing access group, select it from the list and click the pencil icon (Modify).

Deleting access groups

Use the Fibre Channel tab to delete access groups.

Procedure

1. Go to **Data Management > DD Boost > Fibre Channel**.
2. Select the group to be deleted from the DD Boost Access Groups list.

Note

You cannot delete a group that has initiators assigned to it. Edit the group to remove the initiators first.

3. Click Delete (X).

About the DD Boost tabs

Learn to use the DD Boost tabs in System Manager.

Settings

Use the Settings tab to enable or disable DD Boost, select clients and users, and specify advanced options.

The Settings tab shows the DD Boost status (Enabled or Disabled). Use the **Status** button to switch between **Enabled** or **Disabled**.

Under **Allowed Clients**, select the clients that are to have access to the system. Use the **Add**, **Modify**, and **Delete** buttons to manage the list of clients.

Under **Users with DD Boost Access**, select the users that are to have DD Boost access. Use the **Add**, **Change Password**, and **Remove** buttons to manage the list of users.

Expand **Advanced Options** to see which advanced options are enabled. Go to **More Tasks > Set Options** to reset these options.

Checking activities

Use the Active Connections tab to see information about clients, interfaces, and outbound files.

Table 121 Connected client information

Item	Description
Client	The name of the connected client.
Idle	Whether the client is idle (Yes) or not (No).
CPUs	The number of CPUs that the client has, such as 8.
Memory (GiB)	The amount of memory (in GiB) the client has, such as 7.8.

Table 121 Connected client information (continued)

Item	Description
Plug-In Version	The DD Boost plug-in version installed, such as 2.2.1.1.
OS Version	The operating system version installed, such as Linux 2.6.17-1.2142_FC4smp x86_64.
Application Version	The backup application version installed, such as NetBackup 6.5.6.
Encrypted	Whether the connection is encrypted (Yes) or not (No).
DSP	Whether or not the connection is using Distributed Segment Processing (DSP) or not.
Transport	Type of transport being used, such as IPv4, IPv6 or DFC (Fibre Channel).

Table 122 Configured interface connection information

Item	Description
Interface	The IP address of the interface.
Interface Group	One of the following: <ul style="list-style-type: none"> The name of the interface group. None, if not a member of one.
Backup	The number of active backup connections.
Restore	The number of active restore connections.
Replication	The number of active replication connections.
Synthetic	The number of synthetic backups.
Total	The total number of connections for the interface.

Table 123 Outbound file replication information

Outbound files item	Description
File Name	The name of the outgoing image file.
Target Host	The name of the host receiving the file.
Logical Bytes to Transfer	The number of logical bytes to be transferred.
Logical Bytes Transferred	The number of logical bytes already transferred.
Low Bandwidth Optimization	The number of low-bandwidth bytes already transferred.

Checking interface groups and clients

The IP Network tab lists configured interface groups. Details include whether or not a group is enabled and any configured client interfaces. Administrators can use the Interface Group menu to view which clients are associated with an interface group.

Checking storage units

Use the Storage Unit tab to create, modify, and delete storage units. To see detailed information about a listed storage unit, select its name.

Table 124 Storage unit: Detailed information

Item	Description
Existing Storage Units	
Storage Unit Name	The name of the storage unit.
Pre-Comp Used	The amount of pre-compressed storage already used.
Pre-Comp Soft Limit	Current value of soft quota set for the storage unit.
% of Pre-Comp Soft Limit Used	Percentage of hard limit quota used.
Pre-Comp Hard Limit	Current value of hard quota set for the storage unit.
% of Pre-Comp Hard Limit Used	Percentage of hard limit quota used.
Storage Unit Details	Select the storage unit in the list.
Total Files	The total number of file images on the storage unit.
Download Files	Link to download storage unit file details in .tsv format. You must allow pop-ups to use this function.
Compression Ratio	The compression ratio achieved on the files.
Metadata Size	The amount of space used for metadata information.
Storage Unit Status	The current status of the storage unit (combinations are supported). Status can be: <ul style="list-style-type: none"> • D—Deleted • RO—Read-only • RW—Read/write • RD—Replication destination • RLE—Retention lock enabled • RLD—Retention lock disabled
Quota Enforcement	Click Quota to go to the Data Management Quota page, which lists hard and soft quota values/percentage used by MTrees.
Quota Summary	Percentage of Hard Limit used.
Original Size	The size of the file before compression was performed.
Global Compression Size	The total size after global compression of the files in the storage unit when they were written.
Locally Compressed Size	Total size after local compression of the files in the storage unit when they were written.

CHAPTER 12

DD Virtual Tape Library

This chapter includes:

- [DD Virtual Tape Library overview](#) 280
- [Planning a VTL](#).....280
- [Managing a VTL](#)..... 284
- [Working with libraries](#)..... 287
- [Working with a selected library](#).....291
- [Viewing changer information](#) 298
- [Working with drives](#) 299
- [Working with a selected drive](#)..... 301
- [Working with tapes](#) 301
- [Working with the vault](#).....303
- [Working with pools](#).....303
- [Working with a selected pool](#).....305

DD Virtual Tape Library overview

EMC Data Domain Virtual Tape Library (VTL) is a disk-based backup system that emulates the use of physical tapes. It enables backup applications to connect to and manage DD system storage using functionality almost identical to a physical tape library.

Virtual tape drives are accessible to backup software in the same way as physical tape drives. After you create these drives in a VTL, they appear to the backup software as SCSI tape drives. The VTL, itself, appears to the backup software as a SCSI robotic device accessed through standard driver interfaces. However, the movement of the media changer and backup images is managed by the backup software – not by the DD system configured as a VTL.

The following terms have special meaning when used with VTL:

- *Library* – A library emulates a physical tape library with drives, changer, CAPs (cartridge access ports), and slots (cartridge slots).
- *Tape* – A tape is represented as a file. Tapes can be imported from the vault to a library. Tapes can be exported from a library to the vault. Tapes can be moved within a library across drives, slots, and CAPs.
- *Pool* – A pool is a collection of tapes that maps to a directory on the file system. Pools are used to replicate tapes to a destination. You can convert directory-based pools to MTree-based pools to take advantage of the greater functionality of MTrees.
- *Vault* – The vault holds tapes not being used by any library. Tapes reside in either a library or the vault.

VTL has been tested with, and is supported by, specific backup software and hardware configurations. For more information, see the appropriate *Backup Compatibility Guide* on the EMC Online Support Site.

VTL supports simultaneous use of the tape library and file system (NFS/CIFS/DD Boost) interfaces.

When DR (disaster recovery) is needed, pools and tapes can be replicated to a remote DD system using the DD Replicator.

To protect data on tapes from modification, tapes can be locked using Retention Lock Governance software.

Note

At present, for 16 Gb/s, EMC supports fabric and point-to-point topologies; other topologies will present issues.

Planning a VTL

The VTL (Virtual Tape Library) feature has very specific requirements, such as proper licensing, interface cards, user permissions, etc. These requirements are listed here, complete with details and recommendations.

- An appropriate VTL license.
 - VTL is a licensed feature, and you must use NDMP (Network Data Management Protocol) over IP (Internet Protocol) or VTL directly over FC (Fibre Channel).
 - An additional license is required for IBM i systems – the I/OS license.
 - Adding a VTL license through the DD System Manager automatically disables and enables the VTL feature.

- An installed FC interface card or VTL configured to use NDMP.
 - If the VTL communication between a backup server and a DD system is through an FC interface, the DD system must have an FC interface card installed. Notice that whenever an FC interface card is removed from (or changed within) a DD system, any VTL configuration associated with that card must be updated.
 - If the VTL communication between a backup server and a DD system is through NDMP, no FC interface card is required. However, you must configure the TapeServer access group. Also, when using NDMP, all initiator and port functionality does not apply.
- A backup software minimum record (block) size.
 - EMC strongly recommends that backup software be set to use a minimum record (block) size of 64 KiB or larger. Larger sizes usually give faster performance and better data compression.
 - Depending on your backup application, if you change the size after the initial configuration, data written with the original size might become unreadable.
- Appropriate user access to the system.
 - For basic tape operations and monitoring, only a user login is required.
 - To enable and configure VTL services and perform other configuration tasks, a sysadmin login is required.

VTL limits

Before setting up or using a VTL, review these limits on size, slots, etc.

- I/O Size – The maximum supported I/O size for any DD system using VTL is 1 MB.
- Libraries – VTL supports a maximum of 64 libraries per DD system (that is, 64 VTL instances on each DD system).
- Initiators – VTL supports a maximum of 1024 initiators or WWPNs (world-wide port names) per DD system.
- Tape Drives – Information about tape drives is presented in the next section.
- Data Streams – Information about data streams is presented in the section, *Data Streams Sent to a Data Domain System*, in the File System chapter.
- Slots – VTL supports a maximum of:
 - 32,000 slots per library
 - 64,000 slots per DD system

The DD system automatically adds slots to keep the number of slots equal to, or greater than, the number of drives.

Note

Some device drivers (for example, IBM AIX atape device drivers) limit library configurations to specific drive/slot limits, which may be less than what the DD system supports. Backup applications, and drives used by those applications, may be affected by this limitation.

- CAPs (cartridge access ports) – VTL supports a maximum of:
 - 100 CAPs per library
 - 1000 CAPs per DD system

Number of drives supported by a VTL

The maximum number of drives supported by a VTL depends on the number of CPU cores and the amount of memory installed (both RAM and NVRAM, if applicable) on a DD system.

Note

There are no references to model numbers in this table because there are many combinations of CPU cores and memories for each model, and the number of supported drives depends *only* on the CPU cores and memories – not on the particular model, itself.

Table 125 Number of drives supported by a VTL

Number of CPU cores	RAM (in GB)	NVRAM (in GB)	Maximum number of supported drives
Fewer than 32	4 or less	NA	64
	More than 4, up to 38	NA	128
	More than 38, up to 128	NA	256
	More than 128	NA	540
32 to 39	Up to 128	Less than 4	270
	Up to 128	4 or more	540
	More than 128	NA	540
40 to 59	NA	NA	540
60 or more	NA	NA	1080

Tape barcodes

When you create a tape, you must assign a barcode as a unique identifier. Never use duplicate barcodes because this can cause unpredictable behavior. Each barcode consists of eight characters: the first six are numbers or uppercase letters (0-9, A-Z), and the last two are the tape code for the supported tape type, as shown in the following table.

Table 126 Tape Codes by Tape Type

Tape Type	Default Capacity (unless noted)	Tape Code
LTO-1	100 GiB	L1
LTO-1	50 GiB (non-default)	LA ^a
LTO-1	30 GiB (non-default)	LB
LTO-1	10 GiB (non-default)	LC
LTO-2	200 GiB	L2

Table 126 Tape Codes by Tape Type (continued)

Tape Type	Default Capacity (unless noted)	Tape Code
LTO-3	400 GiB	L3
LTO-4	800 GiB	L4
LTO-5 (default)	1.5 TiB	L5

- a. For TSM, use the L2 tape code if the LA code is ignored.

For multiple tape libraries, barcodes are automatically incremented, if the sixth character (just before the "L") is a number. If an overflow occurs (9 to 0), numbering moves one position to the left. If the next character to increment is a letter, incrementation stops.

Here are a few sample barcodes and how each will be incremented:

- 000000L1 creates tapes of 100 GiB capacity and can accept a count of up to 100,000 tapes (from 000000 to 99999).
- AA0000LA creates tapes of 50 GiB capacity and can accept a count of up to 10,000 tapes (from 0000 to 9999).
- AAAA00LB creates tapes of 30GiB capacity and can accept a count of up to 100 tapes (from 00 to 99).
- AAAAAALC creates one tape of 10 GiB capacity. Only one tape can be created with this name.
- AAA350L1 creates tapes of 100 GiB capacity and can accept a count of up to 650 tapes (from 350 to 999).
- 000AAALA creates one tape of 50 GiB capacity. Only one tape can be created with this name.
- 5M7Q3KLB creates one tape of 30 GiB capacity. Only one tape can be created with this name.

LTO tape drive compatibility

You may have different generations of LTO (Linear Tape-Open) technology in your setup; the compatibility between these generations is presented in tabular form.

In this table:

- RW = read and write compatible
- R = read-only compatible
- — = not compatible

Table 127 LTO tape drive compatibility

tape format	LTO-5	LTO-4	LTO-3	LTO-2	LTO-1
LTO-5	RW				
LTO-4	RW	RW	—	—	—
LTO-3	R	RW	RW	—	—
LTO-2		R	RW	RW	—
LTO-1		—	R	RW	RW

Table 127 LTO tape drive compatibility (continued)

Setting up a VTL

To set up a simple VTL, use the Configuration Wizard, which is described in the *Getting Started* chapter.

Similar documentation is available in the *EMC Data Domain Operating System Initial Configuration Guide*.

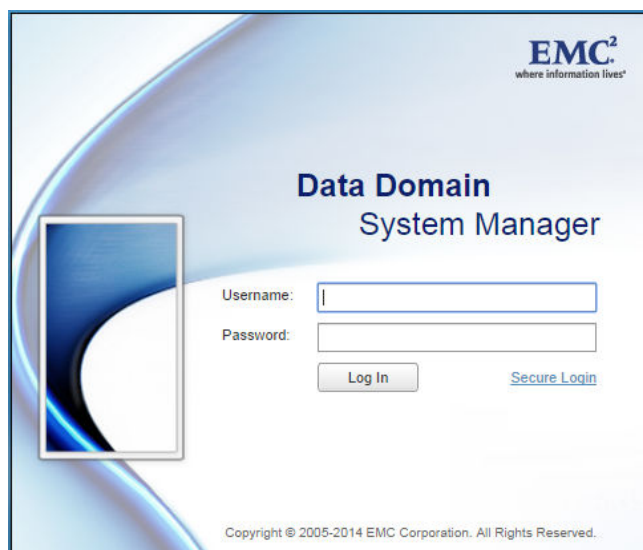
Then, continue with the following topics to enable the VTL, create libraries, and create and import tapes.

Managing a VTL

You can manage a VTL using the DD System Manager or using the Command Line Interface (CLI). After you login, you can check the status of your VTL process, check your license information, and review and configure options.

Logging In

To manage a Virtual Tape Library (VTL), log in to the DD System Manager.



CLI Equivalent

You can also log in at the CLI:

```
login as: sysadmin
Data Domain OS 5.5.x.x-12345
Using keyboard-interactive authentication.
Password:
```

Enabling SCSI Target Daemon (CLI only)

If you do log in from the CLI, you must enable the `scsitarget` daemon (the Fibre Channel service). This daemon is enabled during the VTL or DD Boost-FC enable selections in DD System Manager. In the CLI, these processes need to be enabled separately.

```
# scsitarget enable
Please wait ...
SCSI Target subsystem is enabled.
```

Selecting a DD System

Select a DD system from the DD Network on the left. Then, select **Data Management** > **VTL** > **Virtual Tape Libraries** > **VTL Service**.

[There are additional areas for working with tape storage – Access Groups, Physical Resources, and Pools – which are described in other parts of this guide.]

VTL Process Status

The status of your VTL process is displayed at the top, for example, **Enabled: Running**. The first part of the status will be **Enabled** (on) or **Disabled** (off). The second part will be one of the following states.

Table 128 VTL process states

State	Description
Running	VTL process is enabled and active (shown in green).
Starting	VTL process is starting.
Stopping	VTL process is being shut down.
Stopped	VTL process is disabled (shown in red).
Timing out	VTL process crashed and is attempting an automatic restart.
Stuck	After several failed automatic restarts, the VTL process is unable to shut down normally, so an attempt is being made to kill it.

VTL License

All license information should be populated as part of the factory configuration process; however, based on the timing of the purchase of the VTL option, the VTL license key may not have been populated in the DD system.

The VTL license line tells you whether your VTL license has been applied. If it says **Unlicensed**, select **Add License**. Enter your license key in the Add License Key dialog. Select **Next** and **OK**.

CLI Equivalent

You can also verify that the VTL license has been installed at the CLI:

```
# license show
## License Key                               Feature
--
1      DEFA-EFCD-FCDE-CDEF                   Replication
2      EFCD-FCDE-CDEF-DEFA                   VTL
--
```

If the license is not present, each unit comes with documentation – a quick install card – which will show the licenses that have been purchased. Enter the following command to populate the license key.

```
# license add license-code
```

VTL Options Tab

The Options tab displays the following information.

Table 129 Options tab

Item	Description
Property	Lists the configured options:

Table 129 Options tab (continued)

Item	Description
	<ul style="list-style-type: none"> • auto-eject • auto-offline • I/OS License (for IBM i customers)
Value	<p>Provides the value for each configured option:</p> <ul style="list-style-type: none"> • auto-eject – The state, either enabled or disabled. • auto-offline – The state, either enabled or disabled. When enabled, automatically takes a drive offline before a tape move operation is performed. • I/OS License – Displays the I/OS license. Select Add License to add a license for I/OS.

Configure

Select the Configure button to change the value of these options.

Detailed Information

The next topics provide more details on how to enable and disable VTL, as well as how to configure certain options.

Enabling VTL

Enabling VTL broadcasts the WWN of the Data Domain HBA to customer fabric and enables all libraries and library drives. If a forwarding plan is required in the form of change control processes, this process should be enabled to facilitate zoning.

Procedure

1. Make sure you have a VTL license.
2. Select **Virtual Tape Libraries > VTL Service**.
3. To the right of the Status area, select **Enable**.
4. In the Enable Service dialog, select **OK**.
5. After VTL has been enabled, note that Status will change to **Enabled: Running** in green. Also note that the configured VTL options are displayed in the Options tab.

CLI Equivalent

```
# vtl enable
Starting VTL, please wait ...
VTL is enabled.
```

Disabling VTL

Disabling VTL closes all libraries and shuts down the VTL process.

Procedure

1. Select **Virtual Tape Libraries > VTL Service**.
2. To the right of the Status area, select **Disable**.

3. In the Disable Service dialog, select **OK**.
4. After VTL has been disabled, notice that the Status has changed to **Disabled: Stopped** in red.

CLI Equivalent

```
# vtl disable
```

Configuring VTL service options

VTL service options include enabling or disabling auto-eject and/or auto-offline.

Enabling auto-eject causes any tape put into a CAP (cartridge access port) to automatically move to the virtual vault, unless:

- the tape came from the vault, in which case the tape stays in the CAP.
- an `ALLOW_MEDIUM_REMOVAL` command with a 0 value (false) has been issued to the library to prevent the removal of the medium from the CAP to the outside world.

Enabling auto-offline takes a drive offline automatically before a tape move operation is performed.

Note that customers of IBM i must enter a valid I/OS license in either of these formats: `xxxx-xxxx-xxxx-xxxx` or `xxxx-xxxx-xxxx-xxxx-xxxx`. This I/OS license must be installed before creating the library and drives to be used on the IBM i system.

You can configure VTL service options when you add a license, or any time thereafter.

Procedure

1. Select **Virtual Tape Libraries > VTL Service**.
2. To the right of the VTL License area, select **Add License**.
3. In the Add License Key dialog, enter a valid license key number.
4. Select **Next**.
5. Under the Options tab, select **Configure** to see the Configure Option dialog.
 - a. For auto-eject, select **Enable**.
 - b. For auto-offline, select **Enable**.
 - c. Select **OK**.
6. To disable all of these service options, select **Reset to Default**.

Working with libraries

A library emulates a physical tape library with drives, changer, CAPs (cartridge access ports), and slots (cartridge slots). Selecting **Virtual Tape Libraries > VTL Service > Libraries** displays detailed information for all configured libraries.

Table 130 Library information

Item	Description
Name	The name of a configured library.
Drives	The number of drives configured in the library.
Slots	The number of slots configured in the library.

Table 130 Library information (continued)

Item	Description
CAPs	The number of CAPs (cartridge access ports) configured in the library.

From the More Tasks menu, you can create and delete libraries, as well as search for tapes.

Creating libraries

VTL supports a maximum of 64 libraries per system, that is, 64 concurrently active virtual tape library instances on each DD system.

Procedure

1. Select **Virtual Tape Libraries** > **VTL Service** > **Libraries**.
2. Select **More Tasks** > **Library** > **Create**
3. In the Create Library dialog, enter the following information:

Table 131 Create Library dialog

Field	User input
Library Name	Enter a name of from 1 to 32 alphanumeric characters.
Number of Drives	Enter the number of drives (from 1 to 98). The number of drives to be created will correspond to the number of data streams that will write to a library.
Drive Model	Select the desired model from the drop-down list: <ul style="list-style-type: none"> • IBM-LTO-1 • IBM-LTO-2 • IBM-LTO-3 • IBM-LTO-4 • IBM-LTO-5 (default) • HP-LTO-3 • HP-LTO-4 Do not mix drive types, or media types, in the same library. This can cause unexpected results and/or errors in the backup operation.
Number of Slots	Enter the number of slots in the library. Here are some things to consider: <ul style="list-style-type: none"> • The number of slots must be equal to or greater than the number of drives. • You can have up to 32,000 slots per individual library • You can have up to 64,000 slots per system. • Try to have enough slots so tapes remain in the VTL and never need to be exported to a vault – to avoid reconfiguring the VTL and to ease management overhead.

Table 131 Create Library dialog (continued)

Field	User input
	<ul style="list-style-type: none"> Consider any applications that are licensed by the number of slots. <p>As an example, for a standard 100-GB cartridge on a DD580, you might configure 5000 slots. This would be enough to hold up to 500 TB (assuming reasonably compressible data).</p>
Number of CAPs	<p>(Optional) Enter the number of cartridge access ports (CAPs).</p> <ul style="list-style-type: none"> You can have up to 100 CAPs per library. You can have up to 1000 CAPs per system. <p>Check your particular backup software application documentation on the EMC Online Support Site for guidance.</p>
Changer Model Name	<p>Select the desired model from the drop-down list:</p> <ul style="list-style-type: none"> L180 (default) RESTORER-L180 TS3500 (which should be used for IBMi deployments) I2000 I6000 DDVTL <p>Check your particular backup software application documentation on the EMC Online Support Site for guidance. Also refer to the VTL support matrix to see the compatibility of emulated libraries to supported software.</p>

4. Select **OK**.

After the Create Library status dialog shows **Completed**, select **OK**.

The new library appears under the Libraries icon in the VTL Service tree, and the options you have configured appear as icons under the library. Selecting the library displays details about the library in the Information Panel.

Note that access to VTLs and drives is managed with Access Groups.

CLI Equivalent

```
# vtl add NewVTL model L180 slots 50 caps 5
```

This adds the VTL library, NewVTL. Use 'vtl show config NewVTL' to view it.

```
# vtl drive add NewVTL count 4 model IBM-LTO-3
```

This adds 4 IBM-LTO-3 drives to the VTL library, NewVTL.

Deleting libraries

When a tape is in a drive within a library, and that library is deleted, the tape is moved to the vault. However, the tape's pool does not change.

Procedure

1. Select **Virtual Tape Libraries** > **VTL Service** > **Libraries**.
2. Select **More Tasks** > **Library** > **Delete**.
3. In the Delete Libraries dialog, select or confirm the checkbox of the items to delete:
 - The name of each library, or
 - Library Names, to delete all libraries
4. Select **Next**.
5. Verify the libraries to delete, and select **Submit** in the confirmation dialogs.
6. After the Delete Libraries Status dialog shows **Completed**, select **Close**. The selected libraries are deleted from the VTL.

CLI Equivalent

```
# vtl del OldVTL
```

Searching for tapes

You can use a variety of criteria – location, pool, and/or barcode – to search for a tape.

Procedure

1. Select **Virtual Tape Libraries** or **Pools**.
2. Select the area to search (library, vault, pool).
3. Select **More Tasks** > **Tapes** > **Search**.
4. In the Search Tapes dialog, enter information about the tape(s) you want to find.

Table 132 Search Tapes dialog

Field	User input
Location	Specify a location, or leave the default (All).
Pool	Select the name of the pool in which to search for the tape. If no pools have been created, use the Default pool.
Barcode	Specify a unique barcode. or leave the default (*) to return a group of tapes. Barcode allows the wildcards ? and *, where ? matches any single character and * matches 0 or more characters.
Count	Enter the maximum number of tapes you want to be returned to you. If you leave this blank, the barcode default (*) is used.

5. Select **Search**.

Working with a selected library

Selecting **Virtual Tape Libraries** > **VTL Service** > **Libraries** > *library* displays detailed information for a selected library.

Table 133 Devices

Item	Description
Device	The elements in the library, such as drives, slots, and CAPs (cartridge access ports).
Loaded	The number of devices with media loaded.
Empty	The number of devices with no media loaded.
Total	The total number of loaded and empty devices.

Table 134 Tapes

Item	Description
Pool	The name of the pool where the tapes are located.
Tape Count	The number of tapes in that pool.
Capacity	The total configured data capacity of the tapes in that pool, in GiB (Gibibytes, the base-2 equivalent of GB, Gigabytes).
Used	The amount of space used on the virtual tapes in that pool.
Average Compression	The average amount of compression achieved on the data on the tapes in that pool.

From the More Tasks menu, you can perform tasks for the library, and work with the tapes, slots and CAPs in the library.

Creating tapes

You can create tapes in either a library or a pool. If initiated from a pool, the system first creates the tapes, then imports them to the library.

Procedure

1. Select **Virtual Tape Libraries** > **Libraries** > *library* or **Vault** or **Pools** > **Pools** > *pool*.
2. Select **More Tasks** > **Tapes** > **Create**.
3. In the Create Tapes dialog, enter the following information about the tape:

Table 135 Create Tapes dialog

Field	User input
Library (if initiated from a library)	If a drop-down menu is enabled, select the library or leave the default selection.

Table 135 Create Tapes dialog (continued)

Field	User input
Pool Name	Select the name of the pool in which the tape will reside, from the drop-down list. If no pools have been created, use the Default pool.
Number of Tapes	For a library, select from 1 to 20. For a pool, select from 1 to 100,000, or leave the default (20). [Although the number of supported tapes is unlimited, you can create no more than 100,000 tapes at a time.]
Starting Barcode	Enter the initial barcode number (using the format A99000LA).
Tape Capacity	(optional) Specify the number of GiBs from 1 to 4000 for each tape (this setting overrides the barcode capacity setting). For efficient use of disk space, use 100 GiB or fewer.

4. Select **OK** and **Close**.

CLI Equivalent

```
# vtl tape add A00000L1 capacity 100 count 5 pool VTL_Pool
... added 5 tape(s)...
```

Note

You must auto-increment tape volume names in base10 format.

Deleting tapes

You can delete tapes from either a library or a pool. If initiated from a library, the system first exports the tapes, then deletes them. The tapes must be in the vault, not in a library. On a Replication destination DD system, deleting a tape is not permitted.

Procedure

1. Select **Virtual Tape Libraries** > **Libraries** > *library* or **Vault** or **Pools** > **Pools** > *pool*.
2. Select **More Tasks** > **Tapes** > **Delete**.
3. In the Delete Tapes dialog, enter search information about the tapes to delete, and select **Search**:

Table 136 Delete Tapes dialog

Field	User input
Location	If there is a drop-down list, select a library, or leave the default Vault selection.
Pool	Select the name of the pool in which to search for the tape. If no pools have been created, use the Default pool.
Barcode	Specify a unique barcode, or leave the default (*) to search for a group of tapes. Barcode allows the wildcards ? and *, where ? matches any single character and * matches 0 or more characters.
Count	Enter the maximum number of tapes you want to be returned to you. If you leave this blank, the barcode default (*) is used.

Table 136 Delete Tapes dialog (continued)

Field	User input
Tapes Per Page	Select the maximum number of tapes to display per page – possible values are 15, 30, and 45.
Select all pages	Select the Select All Pages checkbox to select all tapes returned by the search query.
Items Selected	Shows the number of tapes selected across multiple pages – updated automatically for each tape selection.

- Select the checkbox of the tape that should be deleted or the checkbox on the heading column to delete all tapes, and select **Next**.
- Select **Submit** in the confirmation window, and select **Close**.

Note

After a tape is removed, the physical disk space used for the tape is not reclaimed until after a file system cleaning operation.

CLI Equivalent

```
# vtl tape del barcode [count count] [pool pool]
```

For example:

```
# vtl tape del A00000L1
```

Note

You can act on ranges; however, if there is a missing tape in the range, the action will stop.

Importing tapes

Importing a tape means that an existing tape will be moved from the vault to a library slot, drive, or cartridge access port (CAP).

The number of tapes you can import at one time is limited by the number of empty slots in the library, that is, you cannot import more tapes than the number of currently empty slots.

To view the available slots for a library, select the library from the stack menu. The information panel for the library shows the count in the Empty column.

- If a tape is in a drive, and the tape origin is known to be a slot, a slot is reserved.
- If a tape is in a drive, and the tape origin is unknown (slot or CAP), a slot is reserved.
- If a tape is in a drive, and the tape origin is known to be a CAP, a slot is not reserved. (The tape returns to the CAP when removed from the drive.)
- To move a tape to a drive, see the section on moving tapes, which follows.

Procedure

- You can import tapes using either step a. or step b.

- a. Select **Virtual Tape Libraries > Libraries > library**. Then, select **More Tasks > Tapes > Import**. In the Import Tapes dialog, enter search information about the tapes to import, and select **Search**:

Table 137 Import Tapes dialog

Field	User input
Location	If there is a drop-down list, select the location of the tape, or leave the default of Vault .
Pool	Select the name of the pool in which to search for the tape. If no pools have been created, use the Default pool.
Barcode	Specify a unique barcode, or leave the default (*) to return a group of tapes. Barcode allows the wildcards ? and *, where ? matches any single character and * matches 0 or more characters.
Count	Enter the maximum number of tapes you want to be returned to you. If you leave this blank, the barcode default (*) is used.
Tapes Per Page	Select the maximum number of tapes to display per page. Possible values are 15, 30, and 45.
Items Selected	Shows the number of tapes selected across multiple pages – updated automatically for each tape selection.

Based on the previous conditions, a default set of tapes is searched to select the tapes to import. If pool, barcode, or count is changed, select Search to update the set of tapes available from which to choose.

- b. Select **Virtual Tape Libraries > Libraries > library > Changer > Drives > drive > Tapes**. Select tapes to import by selecting the checkbox next to:
- An individual tape, or
 - The **Barcode** column to select all tapes on the current page, or
 - The **Select all pages** checkbox to select all tapes returned by the search query.
- Only tapes showing Vault in the Location can be imported.

Select **Import from Vault**. This button is disabled by default and enabled only if all of the selected tapes are from the Vault.

2. From the Import Tapes: library view, verify the summary information and the tape list, and select **OK**.
3. Select **Close** in the status window.

CLI Equivalent

```
# vtl tape show pool VTL_Pool
Processing tapes...
Barcode  Pool      Location State      Size      Used (%)      Comp ModTime
-----  -
A00000L3 VTL_Pool vault    RW         100 GiB  0.0 GiB (0.00%) 0x 2010/07/16 09:50:41
A00001L3 VTL_Pool vault    RW         100 GiB  0.0 GiB (0.00%) 0x 2010/07/16 09:50:41
A00002L3 VTL_Pool vault    RW         100 GiB  0.0 GiB (0.00%) 0x 2010/07/16 09:50:41
A00003L3 VTL_Pool vault    RW         100 GiB  0.0 GiB (0.00%) 0x 2010/07/16 09:50:41
A00004L3 VTL_Pool vault    RW         100 GiB  0.0 GiB (0.00%) 0x 2010/07/16 09:50:41
-----  -
VTL Tape Summary
-----
```

```

Total number of tapes:      5
Total pools:                1
Total size of tapes:       500 GiB
Total space used by tapes:  0.0 GiB
Average Compression:       0.0x

# vtl import NewVTL barcode A00000L3 count 5 pool VTL_Pool
... imported 5 tape(s)...

# vtl tape show pool VTL_Pool
Processing tapes....

VTL Tape Summary
-----
Total number of tapes:      5
Total pools:                1
Total size of tapes:       500 GiB
Total space used by tapes:  0.0 GiB
Average Compression:       0.0x

```

Exporting tapes

Exporting a tape removes that tape from a slot, drive, or cartridge-access port (CAP) and sends it to the vault.

Procedure

1. You can export tapes using either step a. or step b.
 - a. Select **Virtual Tape Libraries** > **Libraries** > *library*. Then, select **More Tasks** > **Tapes** > **Export**. In the Export Tapes dialog, enter search information about the tapes to export, and select **Search**:

Table 138 Export Tapes dialog

Field	User input
Location	If there is a drop-down list, select the name of the library where the tape is located, or leave the selected library.
Pool	Select the name of the pool in which to search for the tape. If no pools have been created, use the Default pool.
Barcode	Specify a unique barcode. or leave the default (*) to return a group of tapes. Barcode allows the wildcards ? and *, where ? matches any single character and * matches 0 or more characters.
Count	Enter the maximum number of tapes you want to be returned to you. If you leave this blank, the barcode default (*) is used.
Tapes Per Page	Select the maximum number of tapes to display per page. Possible values are 15, 30, and 45.
Select all pages	Select the Select All Pages checkbox to select all tapes returned by the search query.
Items Selected	Shows the number of tapes selected across multiple pages – updated automatically for each tape selection.

- b. Select **Virtual Tape Libraries** > **Libraries** > *library* > **Changer** > **Drives** > *drive* > **Tapes**. Select tapes to export by selecting the checkbox next to:
 - An individual tape, or

- The **Barcode** column to select all tapes on the current page, or
- The **Select all pages** checkbox to select all tapes returned by the search query.

Only tapes with a library name in the Location column can be exported.

Select **Export from Library**. This button is disabled by default and enabled only if all of the selected tapes have a library name in the Location column.

2. From the Export Tapes: library view, verify the summary information and the tape list, and select **OK**.
3. Select **Close** in the status window.

Moving tapes between devices within a library

Tapes can be moved between physical devices within a library to mimic backup software procedures for physical tape libraries (which move a tape in a library from a slot to a drive, a slot to a CAP, a CAP to a drive, and the reverse). In a physical tape library, backup software never moves a tape outside the library. Therefore, the destination library cannot change and is shown only for clarification.

Procedure

1. Select **More Tasks > Tapes > Move**.

Note that when started from a library, the Tapes panel allows tapes to be moved only between devices.

2. In the Move Tape dialog, enter search information about the tapes to move, and select **Search**:

Table 139 Move Tape dialog

Field	User input
Location	Location cannot be changed.
Pool	N/A
Barcode	Specify a unique barcode, or leave the default (*) to return a group of tapes. Barcode allows the wildcards ? and *, where ? matches any single character and * matches 0 or more characters.
Count	Enter the maximum number of tapes you want to be returned to you. If you leave this blank, the barcode default (*) is used.
Tapes Per Page	Select the maximum number of tapes to display per page. Possible values are 15, 30, and 45.
Items Selected	Shows the number of tapes selected across multiple pages – updated automatically for each tape selection.

3. From the search results list, select the tape or tapes to move.
4. Do one of the following:
 - a. Select the device from the Device list (for example, a slot, drive, or CAP), and enter a starting address using sequential numbers for the second and subsequent tapes. For each tape to be moved, if the specified address is occupied, the next available address is used.
 - b. Leave the address blank if the tape in a drive originally came from a slot and is to be returned to that slot; or if the tape is to be moved to the next available slot.

5. Select **Next**.
6. In the Move Tape dialog, verify the summary information and the tape listing, and select **Submit**.
7. Select **Close** in the status window.

Adding slots

You can add slots from a configured library to change the number of storage elements.

Note

Some backup applications do not automatically recognize that slots have been added to a VTL. See your application documentation for information on how to configure the application to recognize this type of change.

Procedure

1. Select **Virtual Tape Libraries** > **Libraries** > *library*.
2. Select **More Tasks** > **Slots** > **Add**.
3. In the Add Slots dialog, enter the Number of Slots to add. The total number of slots in a library, or in all libraries on a system, cannot exceed 32,000 for a library and 64,000 for a system.
4. Select **OK** and **Close** when the status shows *Completed*.

Deleting slots

You can delete slots from a configured library to change the number of storage elements.

Note

Some backup applications do not automatically recognize that slots have been deleted from a VTL. See your application documentation for information on how to configure the application to recognize this type of change.

Procedure

1. If the slot that you want to delete contains cartridges, move those cartridges to the vault. The system will delete only empty, uncommitted slots.
2. Select **Virtual Tape Libraries** > **Libraries** > *library*.
3. Select **More Tasks** > **Slots** > **Delete**.
4. In the Delete Slots dialog, enter the Number of Slots to delete.
5. Select **OK** and **Close** when the status shows *Completed*.

Adding CAPs

You can add CAPs (cartridge access ports) from a configured library to change the number of storage elements.

Note

CAPs are used by a limited number of backup applications. See your application documentation to ensure that CAPs are supported.

Procedure

1. Select **Virtual Tape Libraries** > **Libraries** > *library*.
2. Select **More Tasks** > **CAPs** > **Add**.
3. In the Add CAPs dialog, enter the Number of CAPs to add. You can add from 1 to 100 CAPs per library and from 1 to 1,000 CAPs per system.
4. Select **OK** and **Close** when the status shows *Completed*.

Deleting CAPs

You can delete CAPs (cartridge access ports) from a configured library to change the number of storage elements.

Note

Some backup applications do not automatically recognize that CAPs have been deleted from a VTL. See your application documentation for information on how to configure the application to recognize this type of change.

Procedure

1. If the CAP that you want to delete contains cartridges, move those cartridges to the vault, or this will be done automatically.
2. Select **Virtual Tape Libraries** > **Libraries** > *library*.
3. Select **More Tasks** > **CAPs** > **Delete**.
4. In the Delete CAPs dialog, enter the Number of CAPs to delete. You can delete a maximum of 100 CAPs per library or 1000 CAPs per system.
5. Select **OK** and **Close** when the status shows *Completed*.

Viewing changer information

There can be only one changer per VTL. The changer model you select depends on your specific configuration.

Procedure

1. Select **Virtual Tape Libraries** > **VTL Service** > **Libraries** .
2. Select a specific library.
3. If not expanded, select the plus sign (+) on the left to open the library, and select a Changer element to display the Changer information panel, which provides the following information.

Table 140 Changer information panel

Item	Description
Vendor	The name of the vendor who manufactured the changer
Product	The model name
Revision	The revision level
Serial Number	The changer serial number

Working with drives

Selecting **Virtual Tape Libraries > VTL Service > Libraries > library > Drives** displays detailed information for all drives for a selected library.

Table 141 Drives information panel

Column	Description
Drive	The list of drives by name, where name is “Drive #” and # is a number between 1 and n representing the address or location of the drive in the list of drives.
Vendor	The manufacturer or vendor of the drive, for example, IBM.
Product	The product name of the drive, for example, ULTRIUM-TD5.
Revision	The revision number of the drive product.
Serial Number	The serial number of the drive product.
Status	Whether the drive is Empty, Open, Locked, or Loaded. A tape must be present for the drive to be locked or loaded.
Tape	The barcode of the tape in the drive (if any).
Pool	The pool of the tape in the drive (if any).

Tape and library drivers – To work with drives, you must use the tape and library drivers supplied by your backup software vendor that support the IBM LTO-1, IBM LTO-2, IBM LTO-3, IBM LTO-4, IBM LTO-5 (default), HP-LTO-3, or HP-LTO-4 drives and the StorageTek L180 (default), RESTORER-L180, IBM TS3500, I2000, I6000, or DDVTL libraries. For more information, see the *Application Compatibility Matrices and Integration Guides* for your vendors. When configuring drives, also keep in mind the limits on backup data streams, which are determined by the platform in use.

LTO drive capacities – Because the DD system treats LTO drives as virtual drives, you can set a maximum capacity to 4 TiB (4000 GiB) for each drive type. The default capacities for each LTO drive type are as follows:

- LTO-1 drive: 100 GiB
- LTO-2 drive: 200 GiB
- LTO-3 drive: 400 GiB
- LTO-4 drive: 800 GiB
- LTO-5 drive: 1.5 TiB

Migrating LTO-1 tapes – You can migrate tapes from existing LTO-1 type VTLs to VTLs that include other supported LTO-type tapes and drives. The migration options are different for each backup application, so follow the instructions in the LTO tape migration guide specific to your application. To find the appropriate guide, go to the EMC Online Support Site, and in the search text box, type in **LTO Tape Migration for VTLs**.

Tape full: Early warning – You will receive a warning when the remaining tape space is almost completely full, that is, greater than 99.9, but less than 100 percent. The application can continue writing until the end of the tape to reach 100 percent capacity. The last write, however, is not recoverable.

From the More Tasks menu, you can create or delete a drive.

Creating drives

See the *Number of drives supported by a VTL* section to determine the maximum number of drives supported for your particular VTL.

Procedure

1. Select **Virtual Tape Libraries** > **Libraries** > *library* > **Changer** > **Drives**.
2. Select **More Tasks** > **Drives** > **Create**.
3. In the Create Drive dialog, enter the following information:

Table 142 Create Drive dialog

Field	User input
Location	Select a library name, or leave the name selected.
Number of Drives	See the table in the <i>Number of Drives Supported by a VTL</i> section, earlier in this chapter.
Model Name	Select the model from the drop-down list. If another drive already exists, this option is inactive, and the existing drive type must be used. You cannot mix drive types in the same library. <ul style="list-style-type: none"> • IBM-LTO-1 • IBM-LTO-2 • IBM-LTO-3 • IBM-LTO-4 • IBM-LTO-5 (default) • HP-LTO-3 • HP-LTO-4

4. Select **OK**, and when the status shows *Completed*, select **OK**.

The added drive appears in the Drives list.

Deleting drives

A drive must be empty before it can be deleted.

Procedure

1. If there is a tape in the drive that you want to delete, remove the tape.
2. Select **Virtual Tape Libraries** > **Libraries** > *library* > **Changer** > **Drives**.
3. Select **More Tasks** > **Drives** > **Delete**.
4. In the Delete Drives dialog, select the checkboxes of the drives to delete, or select the **Drive** checkbox to delete all drives.
5. Select **Next**, and after verifying that the correct drive(s) has been selected for deletion, select **Submit**.
6. When the Delete Drive Status dialog shows *Completed*, select **Close**.

The drive will have been removed from the Drives list.

Working with a selected drive

Selecting **Virtual Tape Libraries** > **VTL Service** > **Libraries** > *library* > **Drives** > *drive* displays detailed information for a selected drive.

Table 143 Drive Tab

Column	Description
Drive	The list of drives by name, where name is “Drive #” and # is a number between 1 and n representing the address or location of the drive in the list of drives.
Vendor	The manufacturer or vendor of the drive, for example, IBM.
Product	The product name of the drive, for example, ULTRIUM-TD5.
Revision	The revision number of the drive product.
Serial Number	The serial number of the drive product.
Status	Whether the drive is Empty, Open, Locked, or Loaded. A tape must be present for the drive to be locked or loaded.
Tape	The barcode of the tape in the drive (if any).
Pool	The pool of the tape in the drive (if any).

Table 144 Statistics Tab

Column	Description
Endpoint	The specific name of the endpoint.
Ops/s	The operations per second.
Read KiB/s	The speed of reads in KiB per second.
Write KiB/s	The speed of writes in KiB per second.

From the More Tasks menu, you can delete the drive or perform a refresh.

Working with tapes

A tape is represented as a file. Tapes can be imported from the vault to a library. Tapes can be exported from a library to the vault. Tapes can be moved within a library across drives, slots (cartridge slots), and CAPs (cartridge access ports).

When tapes are created, they are placed into the vault. After they have been added to the vault, they can be imported, exported, moved, searched, or removed.

Selecting **Virtual Tape Libraries** > **VTL Service** > **Libraries** > *library* > **Tapes** displays detailed information for all tapes for a selected library.

Table 145 Tape description

Item	Description
Barcode	The unique barcode for the tape.
Pool	The name of the pool that holds the tape. The Default pool holds all tapes unassigned to a user-created pool.
Location	The location of the tape - whether in a library (and which drive, CAP, or slot number) or in the virtual vault.
State	The state of the tape: <ul style="list-style-type: none"> • RW – Read-writable • RL – Retention-locked • RO – Readable only • WP – Write-protected • RD – Replication destination
Capacity	The total capacity of the tape.
Used	The amount of space used on the tape.
Compression	The amount of compression performed on the data on a tape.
Last Modified	The date of the last change to the tape's information. Modification times used by the system for age-based policies might differ from the last modified time displayed in the tape information sections of the DD System Manager.
Locked Until	If a Retention Lock deadline has been set, the time set is shown. If no retention lock exists, this value is <code>Not specified</code> .

From the information panel, you can import a tape from the vault, export a tape to the library, set a tape's state, create a tape, or delete a tape.

From the More Tasks menu, you can move a tape.

Changing a tape's write or retention lock state

Before changing a tape's write or retention lock state, the tape must have been created and imported. VTL tapes follow the standard Data Domain retention lock policy. After the retention period for a tape has expired, it cannot be written to or changed (however, it can be deleted).

Procedure

1. Select **Virtual Tape Libraries > VTL Service > Libraries > library > Tapes**.
2. Select the tape to modify from the list, and select **Set State** (above the list).
3. In the Set Tape State dialog, select **Read-Writeable**, **Write-Protected**, or **Retention-Lock**.
4. If the state is Retention-Lock, either
 - enter the tape's expiration date in a specified number of days, weeks, months, years, or
 - select the calendar icon, and select a date from the calendar. The Retention-Lock expires at noon on the selected date.

5. Select **Next**, and select **Submit** to change the state.

Working with the vault

The vault holds tapes not being used by any library. Tapes reside in either a library or the vault.

Selecting **Virtual Tape Libraries > VTL Service > Vault** displays detailed information for the Default pool and any other existing pools in the vault.

Table 146 Pool Information

Item	Description
Location	The name of the pool.
Type	Whether it is a Directory or MTree pool.
Tape Count	The number of tapes in the pool.
Capacity	The total amount of space in the pool.
Used	The amount of space used on in the pool.
Average Compression	The average amount of compression in the pool.

From the More Tasks menu, you can create, delete, and search for tapes in the vault.

Working with pools

Selecting **Pools > Pools** displays detailed information for the Default pool and any other existing pools. A *pool* is a collection of tapes that maps to a directory on the file system. Pools are used to replicate tapes to a destination. You can convert directory-based pools to MTree-based pools to take advantage of the greater functionality of MTrees.

Note the following about pools:

- Pools can be of two types: MTree (recommended), or Directory, which is backward-compatible.
- A pool can be replicated no matter where individual tapes are located. Tapes can be in the vault or in a library (slot, cap, or drive).
- You can copy and move tapes from one pool to another.
- Pools are not accessible by backup software.
- No VTL configuration or license is needed on a replication destination when replicating pools.
- You must create tapes with unique barcodes. Duplicate barcodes may cause unpredictable behavior in backup applications and can be confusing to users.
- Two tapes in two different pools on a DD system may have the same name, and in this case, neither tape can be moved to the other tape's pool. Likewise, a pool sent to a replication destination must have a name that is unique on the destination.

Table 147 Pools tab

Item	Description
Location	The location of the pool.

Table 147 Pools tab (continued)

Item	Description
Type	Whether it is a Directory or MTree pool.
Tape Count	The number of tapes in the pool.
Capacity	The total configured data capacity of tapes in the pool, in GiB (Gibibytes base-2 equivalent of GB, Gigabytes).
Used	The amount of space used on virtual tapes in the pool.
Average Compression	The average amount of compression achieved for data on tapes in the pool.

Table 148 Replication tab

Item	Description
Name	The name of the pool.
Configured	Whether replication is configured for the pool: yes or no.
Remote Source	Contains an entry only if the pool is replicated from another DD system.
Remote Destination	Contains an entry only if the pool replicates to another DD system.

From the More Tasks menu, you can create and delete pools, as well as search for tapes.

Creating pools

You can create backward-compatible pools, if necessary for your setup, for example, for replication with a pre-5.2 DD OS system.

Procedure

1. Select **Pools > Pools**.
2. Select **More Tasks > Pool > Create**.
3. In the Create Pool dialog, enter a Pool Name, noting that a pool name:
 - cannot be “all,” “vault,” or “summary.”
 - cannot have a space or period at its beginning or end.
 - is case-sensitive.
4. If you want to create a directory pool (which is backward compatible with the previous version of DD System Manager), select the option “Create a directory backwards compatibility mode pool.” However, be aware that the advantages of using an MTree pool include the ability to:
 - make individual snapshots and schedule snapshots.
 - apply retention locks.
 - set an individual retention policy.
 - get compression information.

- get data migration policies to the Retention Tier.
 - establish a storage space usage policy (quota support) by setting hard limits and soft limits.
5. Select **OK** to display the Create Pool Status dialog.
 6. When the Create Pool Status dialog shows *Completed*, select **Close**. The pool is added to the Pools subtree, and you can now add virtual tapes to it.

CLI Equivalent

```
# vtl pool add VTL_Pool
A VTL pool named VTL_Pool is added.
```

Working with a selected pool

Both **Virtual Tape Libraries** > **VTL Service** > **Vault** > *pool* and **Pools** > **Pools** > *pool* display detailed information for a selected pool. Notice that pool “Default” always exists.

Table 149 Pool Tab

Item	Description
Convert to MTree Pool	Select this button to convert a Directory pool to an MTree pool.
Type	Whether it is a Directory or MTree pool.
Tape Count	The number of tapes in the pool.
Capacity	The total configured data capacity of tapes in the pool, in GiB (Gibibytes, base-2 equivalent of GB, Gigabytes).
Used	The amount of space used on virtual tapes in the pool.
Average Compression	The average amount of compression achieved for data on tapes in the pool.

Table 150 Replication Tab

Item	Description
Name	The name of the pool.
Configured	Whether replication is configured for this pool: yes or no.
Remote Source	Contains an entry only if the pool is replicated from another DD system.
Remote Destination	Contains an entry only if the pool replicates to another DD system.

You can also select the **Replication Detail** button, at the top right, to go directly to the Replication information panel for the selected pool.

In the Vault area, from the More Tasks menu, you can create, delete, move, copy, or search for a tape in the pool.

In the Pools area, from the More Tasks menu, in addition to these tasks, you can also rename or delete a pool.

Converting a directory pool to an MTree pool

MTree pools have many advantages over directory pools. See the *Creating pools* section for more information.

Procedure

1. Make sure the following prerequisites have been met:
 - The source and destination pools must have been synchronized, so that the number of tapes, and the data on each side, remains intact.
 - 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 on multiple systems, those replicating systems must be known to the managing system.
 - 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 DD system.
 - Replicate the directory pool from the second DD system to a third DD system.
 - Remove the second and third DD systems from the managing DD system's Data Domain network.
 - On any of the systems running DD OS 5.5, from the Pools submenu, select **Pools** and a directory pool. In the Pools tab, select **Convert to MTree Pool**.
2. With the directory pool you wish to convert highlighted, choose **Convert to MTree Pool**.
3. Select **OK** in the Convert to MTree Pool dialog.
4. Be aware that conversion affects replication in the following ways:
 - VTL is temporarily disabled on the replicated systems during conversion.
 - The destination data is copied to a new pool on the destination system to preserve the data until the new replication is initialized and synced. Afterward, you may safely delete this temporarily copied pool, which is named **CONVERTED-*pool***, where *pool* is the name of the pool that was upgraded (or the first 18 characters for long pool names). [This applies only to DD OS 5.4.1.0 and later.]
 - The target replication directory will be converted to MTree format. [This applies only to DD OS 5.2 and later.]
 - Replication pairs are broken before pool conversion and re-established afterward if no errors occur.
 - Retention Lock cannot be enabled on systems involved in MTree pool conversion.

Moving tapes between pools

If they reside in the vault, tapes can be moved between pools to accommodate replication activities. For example, pools are needed if all tapes were created in the

Default pool, but you later need independent groups for replicating groups of tapes. You can create named pools and re-organize the groups of tapes into new pools.

Note

You cannot move tapes from a tape pool that is a directory replication source. As a workaround, you can:

- Copy the tape to a new pool, then delete the tape from the old pool.
- Use an MTree pool, which allows you to move tapes from a tape pool that is a directory replication source.

Procedure

1. Select **More Tasks** > **Tapes** > **Move**.

Note that when started from a pool, the Tapes Panel allows tapes to be moved only between pools.

2. In the Move Tapes dialog, enter information to search for the tapes to move, and select **Search**:

Table 151 Move Tapes dialog

Field	User input
Location	Location cannot be changed.
Pool	Select the name of the pool where the tapes reside. If no pools have been created, use the Default pool.
Barcode	Specify a unique barcode. or leave the default (*) to import a group of tapes. Barcode allows the wildcards ? and *, where ? matches any single character and * matches 0 or more characters.
Count	Enter the maximum number of tapes you want to be returned to you. If you leave this blank, the barcode default (*) is used.
Tapes Per Page	Select the maximum number of tapes to display per page. Possible values are 15, 30, and 45.
Items Selected	Shows the number of tapes selected across multiple pages – updated automatically for each tape selection.

3. From the search results list, select the tapes to move.
4. From the Select Destination: Location list, select the location of the pool to which tapes are to be moved. This option is available only when started from the (named) Pool view.
5. Select **Next**.
6. From the Move Tapes view, verify the summary information and tape list, and select **Submit**.
7. Select **Close** in the status window.

Copying tapes between pools

Tapes can be copied between pools, or from the vault to a pool, to accommodate replication activities. This option is available only when started from the (named) Pool view.

Procedure

1. Select **More Tasks** > **Tapes** > **Copy**.
2. In the Copy Tapes Between Pools dialog, select the checkboxes of tapes to copy, or enter information to search for the tapes to copy, and select **Search**:

Table 152 Copy Tapes Between Pools dialog

Field	User input
Location	Select either a library or the Vault for locating the tape. While tapes always show up in a pool (under the Pools menu), they are technically in either a library or the vault, but not both, and they are never in two libraries at the same time. Use the import/export options to move tapes between the vault and a library.
Pool	To copy tapes between pools, select the name of the pool where the tapes currently reside. If no pools have been created, use the Default pool.
Barcode	Specify a unique barcode, or leave the default (*) to import a group of tapes. Barcode allows the wildcards ? and *, where ? matches any single character and * matches 0 or more characters.
Count	Enter the maximum number of tapes you want to be imported. If you leave this blank, the barcode default (*) is used.
Tapes Per Page	Select the maximum number of tapes to display per page. Possible values are 15, 30, and 45.
Items Selected	Shows the number of tapes selected across multiple pages – updated automatically for each tape selection.

3. From the search results list, select the tapes to copy.
4. From the Select Destination: Pool list, select the pool where tapes are to be copied. If a tape with a matching barcode already resides in the destination pool, an error is displayed, and the copy aborts.
5. Select **Next**.
6. From the Copy Tapes Between Pools dialog, verify the summary information and the tape list, and select **Submit**.
7. Select **Close** on the Copy Tapes Between Pools Status window.

Renaming pools

A pool can be renamed only if none of its tapes is in a library.

Procedure

1. Select **Pools** > **Pools***pool* (the pool you wish to rename).
2. Select **More Tasks** > **Pool** > **Rename**.
3. In the Rename Pool dialog, enter the new Pool Name, with the caveat that this name:

- cannot be “all,” “vault,” or “summary.”
 - cannot have a space or period at its beginning or end.
 - is case-sensitive.
4. Select **OK** to display the Rename Pool status dialog.
 5. After the Rename Pool status dialog shows *Completed*, select **Close**.
The pool will have been renamed in the Pools subtree.

Deleting pools

Before a pool can be deleted, you must have deleted any tapes contained within it. If replication is configured for the pool, the replication pair must also be deleted. Deleting a pool corresponds to renaming the MTree and then deleting it, which occurs at the next cleaning process.

Procedure

1. Select **Pools > Pools**.
2. Select **More Tasks > Pool > Delete**.
3. In the Delete Pools dialog, select the checkbox of items to delete:
 - The name of each pool, or
 - **Pool Names**, to delete all pools.
4. Select **Submit** in the confirmation dialogs.
5. When the Delete Pool Status dialog shows *Completed*, select **Close**.
The pool will have been removed from the Pools subtree.

CHAPTER 13

DD Replicator

This chapter includes:

- [DD Replicator overview](#).....312
- [Prerequisites for replication configuration](#)..... 312
- [Replication version compatibility](#)..... 313
- [Using DD Encryption with DD Replicator](#)..... 316
- [Replication types](#)..... 316
- [Replication topologies](#)..... 320
- [Managing replication](#)..... 325
- [Monitoring replication](#) 341

DD Replicator overview

EMC Data Domain Replicator (DD Replicator) provides automated, policy-based, network-efficient, and encrypted replication for DR (disaster recovery) and multi-site backup and archive consolidation. DD Replicator asynchronously replicates only compressed, deduplicated data over a WAN (wide area network).

DD Replicator performs two levels of deduplication to significantly reduce bandwidth requirements: *local* and *cross-site* deduplication. Local deduplication determines the unique segments to be replicated over a WAN. Cross-site deduplication further reduces bandwidth requirements when multiple sites are replicating to the same destination system. With cross-site deduplication, any redundant segment previously transferred by any other site, or as a result of a local backup or archive, will not be replicated again. This improves network efficiency across all sites and reduces daily network bandwidth requirements up to 99%, making network-based replication fast, reliable, and cost-effective.

In order to meet a broad set of DR requirements, DD Replicator provides flexible replication topologies, such as full system mirroring, bi-directional, many-to-one, one-to-many, and cascaded. In addition, you can choose to replicate either all or a subset of the data on your DD system. For the highest level of security, DD Replicator can encrypt data being replicated between DD systems using the standard SSL (Secure Socket Layer) protocol.

DD Replicator scales performance and supported fan-in ratios to support large enterprise environments. When deployed over a 10GB network, DD Replicator can mirror data between two systems at up to 52 TB/hour. In addition, DD Replicator enables up to 270 remote systems to replicate into a single DD990 system, which simplifies administration and reduces costs of DR for remote sites.

Before getting started with DD Replicator, note the following general requirements:

- DD Replicator is a licensed product. See your EMC Data Domain sales representative to purchase licenses.
- You can usually replicate only between machines that are within two releases of each other, for example, from 5.1. to 5.3. However, there may be exceptions to this (as a result of atypical release numbering), so review the tables in the *Replication version compatibility* section, or check with your EMC representative.
- If you are unable to manage and monitor DD Replicator from the current version of the DD System Manager, use the `replication` commands described in the *EMC Data Domain Operating System Command Reference Guide*.

Prerequisites for replication configuration

Before configuring a replication, review the following prerequisites to minimize initial data transfer time, prevent overwriting of data, etc.

- **Contexts** – Determine the maximum number of contexts for your DD systems by reviewing the replication streams numbers in the table in *Data Streams Sent to a Data Domain System*, in the File System chapter.
- **Compatibility** – If you are using DD systems running different versions of DD OS, review the next section on Replication Version Compatibility.
- **Initial Replication** – If the source holds a lot of data, the initial replication operation can take many hours. Consider putting both DD systems in the same location with a high-speed, low-latency link. After the first replication, you can move the systems to their intended locations because only new data will be sent.

- **Bandwidth Delay Settings** – Both the source and destination must have the same bandwidth delay settings. These tuning controls benefit replication performance over higher latency links by controlling the TCP (transmission control protocol) buffer size. The source system can then send enough data to the destination while waiting for an acknowledgment.
- **Only One Context for Directories/Subdirectories** – A directory (and its subdirectories) can be in only one context at a time, so be sure that a subdirectory under a source directory is not used in another directory replication context.
- **Adequate Storage** – At a minimum, the destination must have the *same amount of space* as the source.
- **Destination Empty for Directory Replication** – The destination directory must be empty for directory replication, or its contents no longer needed, because it will be overwritten.

Replication version compatibility

To use DD systems running different versions of DD OS for a source or destination, the following tables provide compatibility information for single-node, extended retention, retention lock, MTree, directory, collection, delta (low bandwidth optimization), and cascaded replication.

In general:

- For DD Boost or OST, see “Optimized Duplication Version Compatibility” in the *Data Domain Boost Administration Guide* for supported configurations.
- MTree and directory replication cannot be used simultaneously for replicating the same data.
- The recovery procedure is valid for all supported replication configurations.
- Migration is supported whenever collection replication is supported.
- MTree replication between a source DD system running DD OS 5.2.x and a destination DD system running DD OS 5.4.x or DD OS 5.5.x is not supported when Retention Lock governance is enabled on the source MTree.
- For cascaded configurations, the maximum number of hops is two, that is, three DD systems.
- One-to-many, many-to-one, and cascaded replication support up to three consecutive DD OS release families, as seen in these figures.

Figure 9 Valid replication configurations

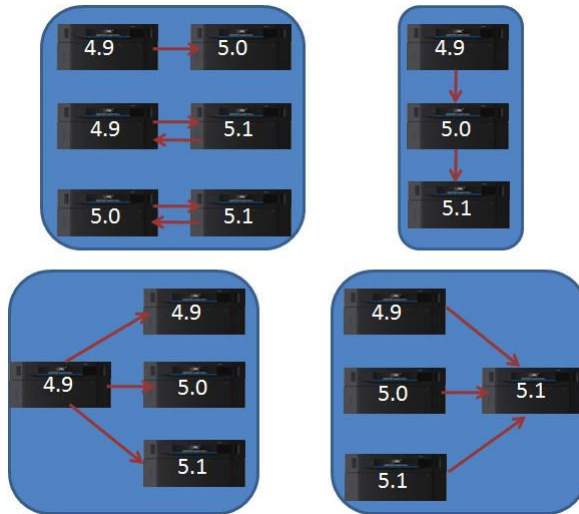


Figure 10 Invalid replication configurations



In these tables:

- Each DD OS release includes all releases in that family, for example, DD OS 5.4 includes 5.4.4.x, 5.4.5.x, etc.
- c = collection replication
- dir = directory replication
- m = MTree replication
- del = delta (low bandwidth optimization) replication
- dest = destination
- src = source
- NA = not applicable

Table 153 Configuration: single-node to single-node

	4.8 (dest)	4.9 (dest)	5.0 (dest)	5.1 (dest)	5.2 (dest)	5.3 (dest)	5.4 (dest)	5.5 (dest)	5.6 (dest)
4.8 (src)	c, dir, del	dir, del	NA	NA	NA	NA	NA	NA	NA
4.9 (src)	NA	c, dir, del	dir, del	dir, del	NA	NA	NA	NA	NA
5.0 (src)	NA	NA	c, dir, del	dir, del	dir, del	NA	NA	NA	NA
5.1 (src)	NA	dir, del	dir, del	c, dir, del, m ^a	dir, del, m ^a	dir, del, m ^a	dir, del, m ^a	NA	NA
5.2 (src)	NA	NA	dir, del	dir, del, m ^a	c, dir, del, m ^b	dir, del, m	dir, del, m	dir, del, m	NA

Table 153 Configuration: single-node to single-node (continued)

	4.8 (dest)	4.9 (dest)	5.0 (dest)	5.1 (dest)	5.2 (dest)	5.3 (dest)	5.4 (dest)	5.5 (dest)	5.6 (dest)
5.3 (src)	NA	NA	NA	dir, del, m ^a	dir, del, m	c, dir, del, m	dir, del, m	dir, del, m	NA
5.4 (src)	NA	NA	NA	dir, del, m ^a	dir, del, m	dir, del, m	c, dir, del, m	dir, del, m	dir, del, m
5.5 (src)	NA	NA	NA	NA	dir, del, m	dir, del, m	dir, del, m	c, dir, del, m	dir, del, m
5.6 (src)	NA	NA	NA	NA	NA	NA	dir, del, m	dir, del, m	c, dir, del, m

- a. MTree replication is unsupported for VTL.
b. Collection replication is supported only for compliance data.

Table 154 Configuration: Extended Retention to Extended Retention

	4.8 (dest)	4.9 (dest)	5.0 (dest)	5.1 (dest)	5.2 (dest)	5.3 (dest)	5.4 (dest)	5.5 (dest)	5.6 (dest)
4.8 (src)	NA	NA	NA	NA	NA	NA	NA	NA	NA
4.9 (src)	NA	NA	NA	NA	NA	NA	NA	NA	NA
5.0 (src)	NA	NA	c	NA	NA	NA	NA	NA	NA
5.1 (src)	NA	NA	NA	c	m ^a	m ^b	m ^b	NA	NA
5.2 (src)	NA	NA	NA	m ^a	c, m ^a	m ^a	m ^a	m ^a	NA
5.3 (src)	NA	NA	NA	m ^c	m ^c	c, m	m	m	NA
5.4 (src)	NA	NA	NA	m ^c	m ^c	m	c, m	m	m
5.5 (src)	NA	NA	NA	NA	m ^c	m	m	c, m	m
5.6 (src)	NA	NA	NA	NA	NA	NA	m	m	c, m

- a. File migration is not supported with MTree replication on either the source or destination in this configuration.
b. File migration is not supported with MTree replication on the source in this configuration.
c. File migration is not supported with MTree replication on the destination in this configuration.

Table 155 Configuration: single-node to Extended Retention

	4.8 (dest)	4.9 (dest)	5.0 (dest)	5.1 (dest)	5.2 (dest)	5.3 (dest)	5.4 (dest)	5.5 (dest)	5.6 (dest)
4.8 (src)	NA	NA	NA	NA	NA	NA	NA	NA	NA
4.9 (src)	NA	NA	NA	NA	NA	NA	NA	NA	NA
5.0 (src)	NA	NA	dir	dir	NA	NA	NA	NA	NA
5.1 (src)	NA	NA	dir	dir, m ^a	dir, m ^a	dir, m	dir, m	NA	NA
5.2 (src)	NA	NA	dir	dir, m ^a	dir, m ^a	dir, m	dir, m	dir, m	NA
5.3 (src)	NA	NA	NA	dir, m ^a	dir, m ^a	dir, m	dir, m	dir, m	NA
5.4 (src)	NA	NA	NA	dir, m ^a	dir, m ^a	dir, m	dir, m	dir, m	dir, m
5.5 (src)	NA	NA	NA	NA	dir, m ^a	dir, m	dir, m	dir, m	dir, m
5.6 (src)	NA	NA	NA	NA	NA	NA	NA	dir, m	dir, m

Table 155 Configuration: single-node to Extended Retention (continued)

- a. File migration is not supported for this configuration.

Using DD Encryption with DD Replicator

DD Replicator can be used with the optional *DD Encryption* feature, enabling encrypted data to be replicated using collection, directory, or MTree replication

Replication contexts are always authenticated with a *shared secret*. That shared secret is used to establish a session key using a Diffie-Hellman key exchange protocol, and that session key is used to encrypt and decrypt the Data Domain system encryption key when appropriate.

Each replication type works uniquely with encryption and offers the same level of security.

- *Collection replication* requires the source and destination to have the same encryption configuration, because the destination data is expected to be an exact replica of the source data. In particular, the encryption feature must be turned on or off at both the source and destination, and if the feature is turned on, the encryption algorithm and the system passphrases must also match. The parameters are checked during the replication association phase.
During collection replication, the source transmits the encrypted user data with the encrypted system encryption key. The data can be recovered at the destination because the destination has the same passphrase and the same system encryption key.
- *MTree or directory replication* does not require encryption configuration to be the same at both the source and destination. Instead, the source and destination securely exchange the destination's encryption key during the replication association phase, and the data is first decrypted and then re-encrypted at the source using the destination's encryption key before transmission to the destination.
If the destination has a different encryption configuration, the data transmitted is prepared appropriately. For example, if the feature is turned off at the destination, the source decrypts the data, and it is sent to the destination un-encrypted.
- In a *cascaded replication* topology, a replica is chained among three Data Domain systems. The last system in the chain can be configured as a collection, MTree, or directory. If the last system is a collection replication destination, it uses the same encryption keys and encrypted data as its source. If the last system is an MTree or directory replication destination, it uses its own key, and the data is encrypted at its source. The encryption key for the destination at each link is used for encryption. Encryption for systems in the chain works as in a replication pair.

Replication types

Replication typically consists of a *source* DD system (which receives data from a backup system) and one or more *destination* DD systems. Each DD system can be the source and/or the destination for replication contexts. During replication, each DD system can perform normal backup and restore operations.

Each replication type establishes a *context* associated with an existing directory or MTree on the source. The replicated context is created on the destination when a context is established. The context establishes a replication pair, which is always active, and any data landing in the source will be copied to the destination at the earliest opportunity.

Paths configured in replication contexts are absolute references and do not change based on the system in which they are configured.

A Data Domain system can be set up for directory, collection, or MTree replication.

- *Directory replication* provides replication at the level of individual directories.
- *Collection replication* duplicates the entire data store on the source and transfers that to the destination, and the replicated volume is read-only.
- *MTree replication* replicates entire MTrees (that is, a virtual file structure that enables advanced management). Media pools can also be replicated, and by default (as of DD OS 5.3), an MTree is created that will be replicated. (A media pool can also be created in backward-compatibility mode that, when replicated, will be a directory replication context.)

For any replication type, note the following requirements:

- A destination Data Domain system must have available storage capacity that is at least the size of the expected maximum size of the source directory. Be sure that the destination Data Domain system has enough network bandwidth and disk space to handle all traffic from replication sources.
- The Data Domain file system must be enabled or, based on the replication type, will be enabled as part of the replication initialization.
- The source must exist.
- The destination must not exist.
- The destination will be created when a context is built and initialized.
- After replication is initialized, ownership and permissions of the destination are always identical to those of the source.
- In the replication command options, a specific replication pair is always identified by the destination.
- Both systems must have an active, visible route through the IP network so that each system can resolve its partner's host name.

The choice of replication type depends on your specific needs. The next sections provide descriptions and features of these three types, plus a brief introduction to Managed File Replication, which is used by DD Boost.

Managed file replication

Managed file replication, which is used by DD Boost, is a type of replication that is managed and controlled by backup software.

With managed file replication, backup images are directly transferred from one DD system to another, one at a time, at the request of the backup software.

The backup software keeps track of all copies, allowing easy monitoring of replication status and recovery from multiple copies.

Managed file replication offers flexible replication topologies including full system mirroring, bi-directional, many-to-one, one-to-many, and cascaded, enabling efficient cross-site deduplication.

Here are some additional points to consider about managed file replication:

- Replication contexts do not need to be configured.
- Lifecycle policies control replication of information with no intervention from the user.
- DD Boost will build and tear down contexts as needed on the fly.

For more information, see the `ddboost file-replication` commands in the *EMC Data Domain Operating System Command Reference Guide*.

Directory replication

Directory replication transfers deduplicated data within a DD file system directory configured as a replication source to a directory configured as a replication destination on a different system.

With directory replication, a DD system can simultaneously be the source of some replication contexts and the destination of other contexts. And that DD system can also receive data from backup and archive applications while it is replicating data.

Directory replication has the same flexible network deployment topologies and cross-site deduplication effects as managed file replication (the type used by DD Boost).

Here are some additional points to consider when using directory replication:

- Do not mix CIFS and NFS data within the same directory. A single destination DD system can receive backups from both CIFS clients and NFS clients as long as separate directories are used for CIFS and NFS.
- Any directory can be in only one context at a time. A parent directory may not be used in a replication context if a child directory of that parent is already being replicated.
- Renaming (moving) files or tapes *into or out of* a directory replication source directory is *not* permitted. Renaming files or tapes *within* a directory replication source directory *is* permitted.
- A destination DD system must have available storage capacity of at least the post-compressed size of the expected maximum post-compressed size of the source directory.
- When replication is initialized, a destination directory is created automatically.
- After replication is initialized, ownership and permissions of the destination directory are always identical to those of the source directory. As long as the context exists, the destination directory is kept in a read-only state and can receive data only from the source directory.
- At any time, due to differences in global compression, the source and destination directory can differ in size.

Folder Creation Recommendations

Directory replication replicates data at the level of individual subdirectories under `/data/col1/backup`.

To provide a granular separation of data you must create, from a host system, other directories (DirA, DirB, etc.) within the `/backup` Mtree. Each directory should be based on your environment and the desire to replicate those directories to another location. You will not replicate the entire `/backup` MTree, but instead would set up replication contexts on each subdirectory underneath `/data/col1/backup/` (ex. `/data/col1/backup/DirC`). The purpose of this threefold:

- It allows control of the destination locations as DirA may go to one site and DirB may go to another.
- This level of granularity allows management, monitoring, and fault isolation. Each replication context can be paused, stopped, destroyed, or reported on.
- Performance is limited on a single context. The creation of multiple contexts can improve aggregate replication performance.

- As a general recommendation, approximately 5 - 10 contexts may be required to distribute replication load across multiple replication streams. This must be validated against the site design and the volume and composition of the data at the location.

Note

Recommending a number of contexts is a design-dependent issue, and in some cases, significant implications are attached to the choices made about segregating data for the purposes of optimizing replication. Data is usually optimized for the manner in which it will rest – not in manner with which it will replicate. Keep this in mind when altering a backup environment.

MTree replication

MTree replication is used to replicate MTrees between DD systems. Periodic snapshots are created on the source, and the differences between them are transferred to the destination by leveraging the same cross-site deduplication mechanism used for directory replication. This ensures that the data on the destination is always a point-in-time copy of the source, with file consistency. This also reduces replication of churn in the data, leading to more efficient utilization of the WAN.

With MTree replication, a DD system can be simultaneously the source of some replication contexts and the destination of other contexts. And that DD system can also receive data from backup and archive applications while it is replicating data.

MTree replication has the same flexible network deployment topologies and cross-site deduplication effects as managed file replication (the type used by DD Boost).

MTree replication replicates data for an MTree specified by the `/data/coll/mtree` pathname.

Here are some additional points to consider when using MTree replication:

- When replication is initialized, a destination read-only MTree is created automatically.
- Data can be logically segregated into multiple MTrees to promote greater replication performance. The current recommendation is no more than 28 concurrently active MTrees (or the limitations of the DD system, if it is fewer).
- Snapshots must be created on source contexts.
- Snapshots cannot be created on a replication destination.
- Snapshots are replicated with a fixed retention of one year; however, the retention is adjustable on the destination and must be adjusted there.
- Archive data movement policies cannot be run on a destination replica MTree.
- Replication contexts must be configured on both the source and the destination.
- Replicating VTL tape cartridges (or pools) simply means replicating MTrees or directories that contain VTL tape cartridges. Media pools are replicated by MTree replication, as a default. A media pool can be created in backward-compatibility mode and can then be replicated via directory-based replication. You cannot use the `pool://` syntax to create replication contexts using the command line. When specifying pool-based replication in DD System Manager, either directory or MTree replication will be created, based on the media pool type.
- Replicating directories under an MTree is not permitted.
- A destination DD system must have available storage capacity of at least the post-compressed size of the expected maximum post-compressed size of the source MTree.

- After replication is initialized, ownership and permissions of the destination MTree are always identical to those of the source MTree. If the context is configured, the destination MTree is kept in a read-only state and can receive data only from the source MTree.
- At any time, due to differences in global compression, the source and destination MTree can differ in size.
- MTree replication is supported from DD Extended Retention systems to non-DD Extended Retention systems if both are running DD OS 5.5 or later.
- Retention Lock Compliance is supported with MTree replication, by default. If Retention Lock is licensed on a source, the destination must also have a Retention Lock license, or replication will fail. (To avoid this situation, you must disable Retention Lock.) If Retention Lock is enabled on a replication context, a replicated destination context will always contain data that is Retention Locked.

Collection replication

Collection replication performs whole-system mirroring in a one-to-one topology, continuously transferring changes in the underlying collection, including all of the logical directories and files of the DD file system.

Collection replication does not have the flexibility of the other types, but it can provide higher throughput and support more objects with less overhead, which may work better for high-scale enterprise cases.

Collection replication replicates the entire `/data/coll` area from a source DD system to a destination DD system.

Here are some additional points to consider when using collection replication:

- No granular replication control is possible. All data is copied from the source to the destination producing a read-only copy.
- Collection replication requires that the storage capacity of the destination system be equal to, or greater than, the capacity of the source system. If the destination capacity is less than the source capacity, the available capacity on the source is reduced to the capacity of the destination.
- The DD system to be used as the collection replication destination must be empty before configuring replication. After replication is configured, this system is dedicated to receive data from the source system.
- With collection replication, all user accounts and passwords are replicated from the source to the destination. However, as of DD OS 5.5.1.0, other elements of configuration and user settings of the DD system are not replicated to the destination; you must explicitly reconfigure them after recovery.
- Retention Lock Compliance supports collection replication.

Replication topologies

DD Replicator supports five replication topologies (one-to-one, one-to-one bidirectional, one-to-many, many-to-one, and cascaded). The tables in this section show (1) how these topologies work with three types of replication (MTree, directory, and collection) and two types of DD systems [single node (SN) and Extended Retention (ER)-enabled] and (2) how mixed topologies are supported with cascaded replication.

In general:

- Single node (SN) systems support all replication topologies.

- Single node-to-single node (SN → SN) can be used for all replication types.
- Extended Retention (ER)-enabled systems cannot be the source for directory replication.
- Collection replication cannot be configured from either a single node (SN) system to an Extended Retention (ER)-enabled system, nor from an ER-enabled system to an SN system.

In this table:

- SN = single node DD system (no Extended Retention)
- ER = Extended Retention-enabled DD system

Table 156 Topology Support by Replication Type and DD System Type

Topologies	MTree Replication	Directory Replication	Collection Replication
one-to-one	{SN ER} → {SN ER} ER→SN [supported starting with 5.5 release; prior to 5.5, it is recovery only]	SN → SN SN → ER	SN → SN ER → ER
one-to-one bidirectional	{SN ER} → {SN ER}	SN → SN	not supported
one-to-many	{SN ER} → {SN ER}	SN → SN SN → ER	not supported
many-to-one	{SN ER} → {SN ER}	SN → SN SN → ER	not supported
cascaded	{SN ER} → {SN ER} → {SN ER}	SN → SN → SN SN → SN → ER	ER → ER → ER SN → SN → SN

Cascaded replication supports mixed topologies where the second leg in a cascaded connection is different from the first type in a connection (for example, A → B is directory replication, and B → C is collection replication).

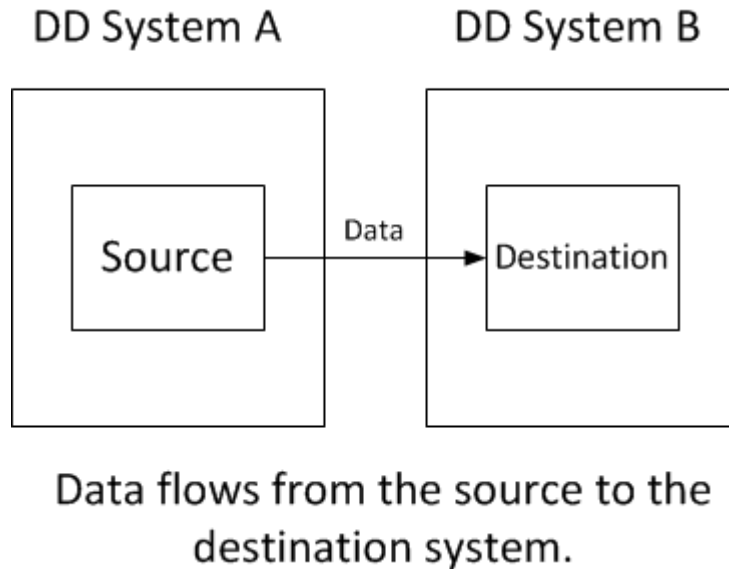
Table 157 Mixed Topologies Supported with Cascaded Replication

Mixed Topologies	
SN – Dir Repl → ER – MTree Repl → ER – MTree Repl	SN – Dir Repl → ER – Col Repl → ER – Col Repl
SN – MTree Repl → SN – Col Repl → SN – Col Repl	SN – MTree Repl → ER – Col Repl → ER – Col Repl

One-to-one replication

The simplest type of replication is from a DD source system to a DD destination system, otherwise known as a *one-to-one* replication pair. This replication topology can be configured with directory, MTree, or collection replication types.

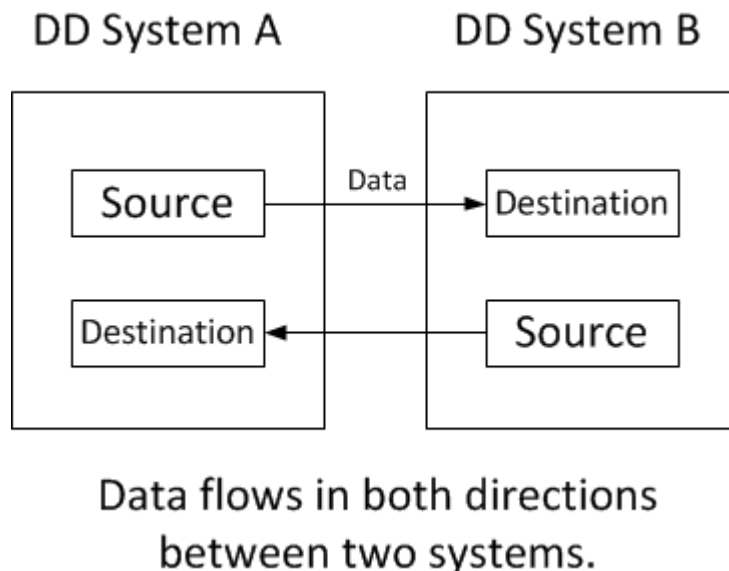
Figure 11 One-to-one replication pair



Bi-directional replication

In a bi-directional replication pair, data from a directory or MTree on DD system A is replicated to DD system B, and from another directory or MTree on DD system B to DD system A.

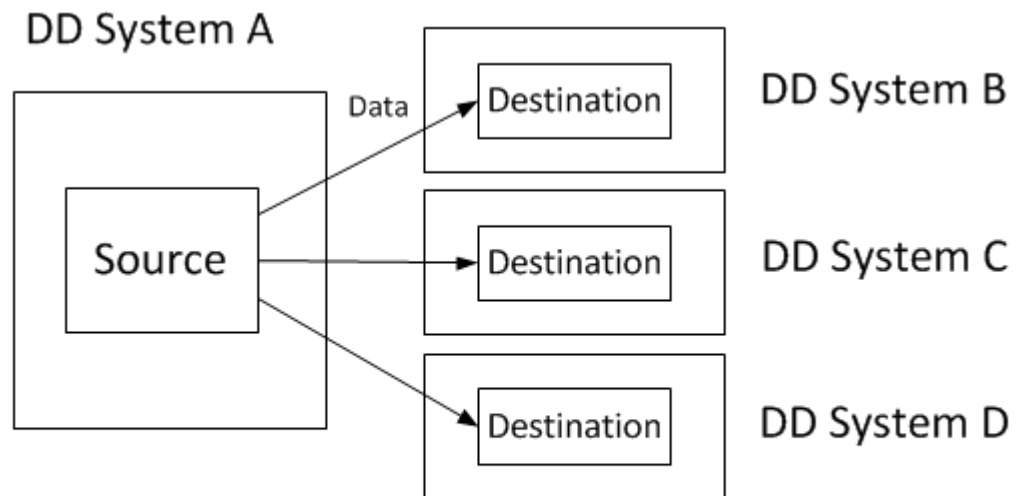
Figure 12 Bi-directional replication



One-to-many replication

In one-to-many replication, data flows from a source directory or MTree on one DD system to several destination DD systems. You could use this type of replication to create more than two copies for increased data protection, or to distribute data for multi-site usage.

Figure 13 One-to-many replication



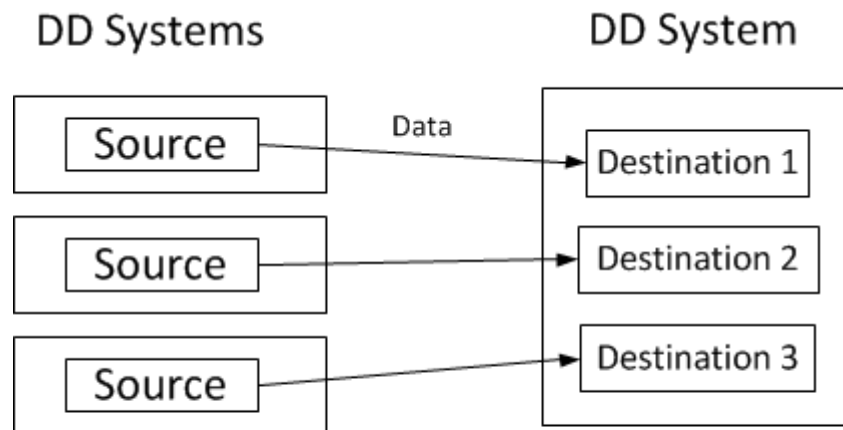
Data flows from a directory or MTree source system to many destination systems.

Many-to-one replication

In many-to-one replication, whether with MTree or directory, replication data flows from several source DD systems to a single destination DD system. This type of replication can

be used to provide data recovery protection for several branch offices on a corporate headquarter's IT system.

Figure 14 Many-to-one replication

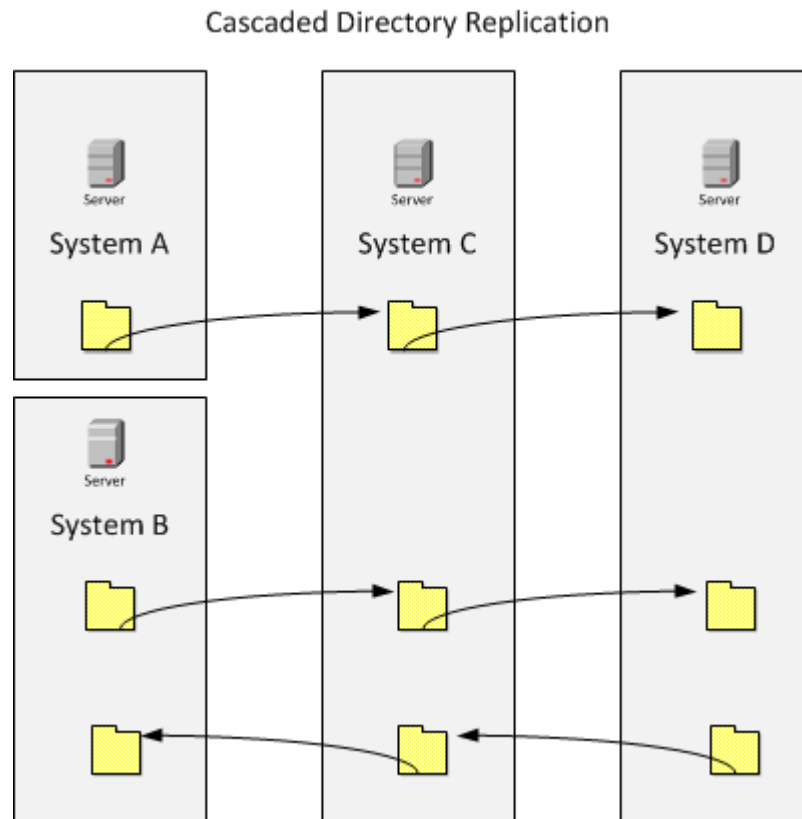


Data flows from many source systems to one destination system.

Cascaded replication

In a cascaded replication topology, a source directory or MTree is chained among three DD systems. The last hop in the chain can be configured as collection, MTree, or directory replication, depending on whether the source is directory or MTree.

For example, DD system A replicates one or more MTrees to DD system B, which then replicates those MTrees to DD system C. The MTrees on DD system B are both a destination (from DD system A) and a source (to DD system C).

Figure 15 Cascaded directory replication

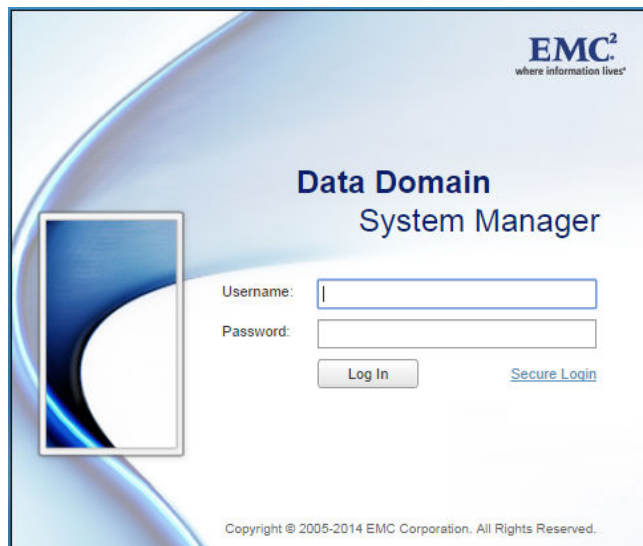
Data recovery can be performed from the non-degraded replication pair context. For example:

- In the event DD system A requires recovery, data can be recovered from DD system B.
- In the event DD system B requires recovery, the simplest method is to perform a replication resync from DD system A to (the replacement) DD system B. In this case, the replication context from DD system B to DD system C should be broken first. After the DD system A to DD system B replication context finishes resync, a new DD system B to DD System C context should be configured and resynced.

Managing replication

Replication is managed by logging into the Data Domain System Manager (DD System Manager) or the CLI. In DD System Manager, the Replication view lets you configure replication pairs and see the configured replicas as a list and as a topology map, check performance graphs, and configure network settings that affect performance.

Start the DD System Manager by logging into your DD system.



To see the Replication view in the DD System Manager:

Procedure

1. Select the source system in the Navigation Panel.
2. Select the Replication tab to access the Replication view.

The Replication Status and the Summary tab are displayed.

3. Select a replication context in the table to populate the Detailed Information.

The next sections describe all of the tabs available in this area. However, if you do *not* have a replication license, you will not see these tabs. (If you have a DD Boost license, you will see the DD Boost tab.) You will simply see a message to the effect that "Replication is not licensed." There is a link in case you *do* have a license and want to add it.

4. If you need to add a destination system, select the Add button above DD Network, and add that system's credentials.

CLI Equivalent

You can also log in at the CLI:

```
login as: sysadmin
Data Domain OS 5.5.x.x-12345
Using keyboard-interactive authentication.
Password:
```

Replication status

Replication Status shows the system-wide count of replication contexts exhibiting a warning (yellow text) or error (red text) state, or if conditions are normal.

Summary view

The Summary view lists the configured replication contexts for a DD system, displaying aggregated information about the selected DD system – that is, summary information

about the inbound and outbound replication pairs. The focus is the DD system, itself, and the inputs to it and outputs from it.

The Summary table can be filtered by entering a Source or Destination name, or by selecting a State (Error, Warning, or Normal).

Table 158 Replication Summary view

Item	Description
Source	System and path name of the source context, with format <i>system.path</i> . For example, for directory <code>dir1</code> on system <code>dd120-22</code> , you would see <code>dd120-22.chaos.local/data/coll/dir1</code> .
Destination	System and path name of destination context, with format <i>system.path</i> . For example, for MTree <code>MTree1</code> on system <code>dd120-44</code> , you would see <code>dd120-44.chaos.local/data/coll/MTree1</code> .
Type	Type of context: MTree, directory (Dir), or Pool.
State	Possible states of replication pair status include: <ul style="list-style-type: none"> • Normal – If the replica is Initializing, Replicating, Recovering, Resyncing, or Migrating. • Idle – For MTree replication, this state can display if the replication process is not currently active or for network errors (such as the destination system being inaccessible). • Warning – If there is an unusual delay for the first five states, or for the Uninitialized state. • Error – Any possible error states, such as Disconnected.
Synced As Of Time	Timestamp for last automatic replication sync operation performed by the source. For MTree replication, this value is updated when a snapshot is exposed on the destination. For directory replication, it is updated when a sync point inserted by the source is applied. A value of unknown displays during replication initialization.
Pre-Comp Remaining	Amount of pre-compressed data remaining to be replicated.
Completion Time (Est.)	Value is either <code>Completed</code> , or the estimated amount of time required to complete the replication data transfer based on the last 24 hours' transfer rate.

Detailed information for a replication context

Selecting one replication context from the Summary view populates that context's information in Detailed Information, Performance Graph, Completion Stats, and Completion Predictor.

Table 159 Detailed Information

Item	Description
State Description	Message about state of replica.

Table 159 Detailed Information (continued)

Item	Description
Source	System and path name of source context, with format <code>system.path</code> . For example, for directory <code>dir1</code> on system <code>dd120-22</code> , you would see <code>dd120-22.chaos.local/data/coll/dir1</code> .
Destination	System and path name of destination context, with format <code>system.path</code> . For example, for MTree <code>MTree1</code> on system <code>dd120-44</code> , you would see <code>dd120-44.chaos.local/data/coll/MTree1</code> .
Connection Port	System name and listen port used for replication connection.

Table 160 Performance Graph

Item	Description
Pre-Comp Remaining	Pre-compressed data remaining to be replicated.
Pre-Comp Written	Pre-compressed data written on the source.
Post-Comp Replicated	Post-compressed data that has been replicated.

Table 161 Completion Stats

Item	Description
Synced As Of Time	Timestamp for last automatic replication sync operation performed by the source. For MTree replication, this value is updated when a snapshot is exposed on the destination. For directory replication, it is updated when a sync point inserted by the source is applied. A value of unknown displays during replication initialization.
Completion Time (Est.)	Value is either <code>Completed</code> or the estimated amount of time required to complete the replication data transfer based on the last 24 hours' transfer rate.
Pre-Comp Remaining	Amount of data remaining to be replicated.
Files Remaining	(Directory Replication Only) Number of files that have not yet been replicated.
Status	For source and destination endpoints, shows status (Enabled, Disabled, Not Licensed, etc.) of major components on the system, such as: <ul style="list-style-type: none"> • Replication • File System • Replication Lock • Encryption at Rest • Encryption over Wire • Available Space

Table 161 Completion Stats (continued)

Item	Description
	<ul style="list-style-type: none"> • Low Bandwidth Optimization • Compression Ratio • Low Bandwidth Optimization Ratio

Completion Predictor

The Completion Predictor is a widget for tracking a backup job's progress and for predicting when replication will complete, for a selected context.

Creating a replication pair

Before creating a replication pair, be sure the destination does not *exist*, or you will get an error.

Procedure

1. Select **Replication** > **Summary** > **Create Pair** to display the Create Pair dialog.
2. Add information to create an MTree, directory, collection, or pool replication pair, as described in the next sections.

Creating a collection replication pair

See the *Collection replication* section for general information about this type of replication.

Before creating a collection replication pair, make sure:

- The storage capacity of the destination system is 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 has been destroyed, and subsequently re-created, but not enabled.
- Each destination and each source is in only one context at a time.
- The file system is disabled on the replica, while configuring and enabling encryption on the source.
- The file system is disabled on the source, while configuring and enabling encryption on the replica.

Procedure

1. In the Create Pair dialog, select **Collection** from the **Replication Type** menu.
2. Select the source system hostname from the **Source System** menu.
3. Select the destination system hostname from the **Destination System** menu. The list includes only those hosts in the DD-Network list.
4. If you want to change any host connection settings, select the **Advanced** tab.
5. Select **OK**. Replication from the source to the destination begins.

Results

Test results from Data Domain returned the following performance guidelines for replication initialization. These are guidelines *only*, and actual performance seen in production environments may vary.

- Over a gigabit LAN: With a high enough shelf count to drive maximum input/output and ideal conditions, collection replication can saturate a 1GigE link (modulo 10% protocol overhead), as well as 400-900 MB/sec on 10GigE, depending on the platform.
- Over a WAN, performance is governed by the WAN link line speed, bandwidth, latency, and packet loss rate.

Creating an MTree, directory, or pool replication pair

See the *MTree replication* and *Directory replication* sections for general information about these types of replication.

When creating an MTree, directory, or pool replication pair:

- Make sure the replication is transiting/exiting the correct interface. When defining a replication context, the host names of the source and destination must resolve with forward and reverse lookups. To make the data transit alternate interfaces on the system, other than the default resolving interface, the replication context must be modified after creation. It may be necessary to set up host files to ensure that contexts are defined on non-resolving (cross-over) interfaces.
- 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-enabled systems to non-Extended Retention-enabled systems, if both are running DD OS 5.5 or later.
- The destination DD 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 DD system can simultaneously be the source for one context and the destination for another context.

Procedure

1. In the Create Pair dialog, select **Directory**, **MTree** (default), or **Pool** from the **Replication Type** menu.
2. Select the source system hostname from the **Source System** menu.
3. Select the destination system hostname from the **Destination System** menu.
4. Enter the source path in the **Source Path** text box (notice the first part of the path is a constant that changes based on the type of replication chosen).
5. Enter the destination path in the **Destination Directory** text box (notice the first part of the path is a constant that changes based on the type of replication chosen).
6. If you want to change any host connection settings, select the **Advanced** tab.
7. Select **OK**.

The Replication from the source to the destination begins.

Test results from Data Domain returned the following guidelines for estimating the time needed for replication initialization.

These are guidelines *only* and may not be accurate in specific production environments.

- Using a T3 connection, 100ms WAN, performance is about 40 MiB/sec of pre-compressed data, which gives data transfer of:

40 MiB/sec = 25 seconds/GiB = 3.456 TiB/day

- Using the base-2 equivalent of gigabit LAN, performance is about 80 MiB/sec of pre-compressed data, which gives data transfer of about double the rate for a T3 WAN.

CLI Equivalent

Here are examples of creating MTree and directory replication pairs at the CLI. The last example specifies the IP version used as a replication transport.

```
# replication add source mtree://ddsource.test.com/data/col1/
examplemtree destination mtree://ddtarget.test.com/data/col1/
examplemtree (Mtree example)
# replication add source dir://ddsource.test.com/data/col1/
directorytorep destination dir://ddtarget.test.com/backup/
directorytorep
# replication add source dir://ddsource.test.com/data/col1/
directorytorep destination dir://ddtarget.test.com/backup/
directorytorep ipversion ipv6
```

To start replication between a source and destination, use the replication initialize command on the source. This command checks that the configuration and connections are correct and returns error messages if any problems appear.

```
# replication initialize mtree://host3.test.com/data/col1/mtree1/
```

Configuring bi-directional replication

To create a bi-directional replication pair, use the directory or MTree replication pair procedure (for example, using mtree2) from host A to host B. Use the same procedure to create a replication pair (for example, using mtree1) from host B to host A. For this configuration, destination pathnames cannot be the same.

Configuring one-to-many replication

To create a one-to-many replication pair, use the directory or MTree replication pair procedure (for example, using mtree1) on host A to: (1) mtree1 on host B, (2) mtree1 on host C, and (3) mtree1 on host D. A replication recovery cannot be done to a source context whose path is the source path for other contexts; the other contexts must be broken and resynced after the recovery.

Configuring many-to-one replication

To create a many-to-one replication pair, use the directory or MTree replication pair procedure [for example, (1) mtree1 from host A to mtree1 on host C and (2) mtree2 on host B to mtree2 on host C.]

Configuring cascaded replication

To create a cascaded replication pair, use the directory or MTree replication pair procedure: (1) mtree1 on host A to mtree1 on host B, and (2) on host B, create a pair for mtree1 to mtree1 on host C. The final destination context (on host C in this example, but more than three hops are supported) can be a collection replica or a directory or MTree replica.

Disabling and enabling a replication pair

Disabling a replication pair temporarily pauses the active replication of data between a source and a destination. The source stops sending data to the destination, and the destination stops serving as an active connection to the source.

Procedure

1. Select one or more replication pairs in the Summary table, and select **Disable Pair**.
2. In the Display Pair dialog, select **Next** and then **OK**.

3. To resume operation of a disabled replication pair, select one or more replication pairs in the Summary table, and select **Enable Pair** to display the Enable Pair dialog.
4. Select **Next** and then **OK**. Replication of data is resumed.

CLI Equivalent

```
# replication disable {destination | all}
# replication enable {destination | all}
```

Deleting a replication pair

When a directory or MTree replication pair is deleted, the destination directory or MTree, respectively, becomes writeable. When a collection replication pair is deleted, the destination DD system becomes a stand-alone read/write system, and the file system is disabled.

Procedure

1. Select one or more replication pairs in the Summary table, and select **Delete Pair**.
2. In the Delete Pair dialog, select **Next** and then **OK**. The replication pairs are deleted.

CLI Equivalent

Before running this command, always run the `filesys disable` command. Then, afterward, run the `filesys enable` command

```
# replication break {destination | all}
```

Changing host connection settings

To direct traffic out of a specific port, modify a current context by altering the connection host parameter using a host name previously defined in the local hosts file to address the alternate system. That host name will correspond to the destination. The host entry will indicate an alternate destination address for that host. This may be required on both the source and destination systems.

Procedure

1. Select the replication pair in the Summary table, and select **Modify Settings**. You can also change these settings when you are performing Create Pair, Start Resync, or Start Recover by selecting the **Advanced** tab.
2. In the Modify Connection Settings dialog, modify any or all of these settings:
 - a. **Use Low Bandwidth Optimization** – For enterprises with small data sets and 6 Mb/s or less bandwidth networks, DD Replicator can further reduce the amount of data to be sent using *low bandwidth optimization*. This enables remote sites with limited bandwidth to use less bandwidth or to replicate and protect more of their data over existing networks. Low bandwidth optimization must be enabled on both the source and destination DD systems. If the source and destination have incompatible low bandwidth optimization settings, low bandwidth optimization will be inactive for that context. After enabling low bandwidth optimization on the source and destination, both systems must undergo a full cleaning cycle to prepare the existing data, so run `filesys clean start` on both systems. The duration of the cleaning cycle depends on the amount of data on the DD system, but takes longer than a normal cleaning. For more information on the `filesys` commands, see the *EMC Data Domain Operating System Command Reference Guide*.

Important: Low bandwidth optimization is not supported if the DD Extended Retention software option is enabled on either DD system. It is also not supported for Collection Replication.

- b. **Enable Encryption Over Wire** – DD Replicator supports encryption of data-in-flight by using standard SSL (Secure Socket Layer) protocol version 3, which uses the ADH-AES256-SHA cipher suite to establish secure replication connections. Both sides of the connection must enable this feature for encryption to proceed.
 - c. **Network Preference** – You may choose IPv4 or IPv6. 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.
 - d. **Use Non-default Connection Host** – The source system transmits data to a destination system listen port. Since a source system can have replication configured for many destination systems (each of which can have a different listen port), each context on the source can configure the connection port to the corresponding listen port of the destination.
3. Select **Next** and then **Close**.

The replication pair settings are updated, and replication resumes.

CLI Equivalent

```
#replication modify <destination> connection-host <new-host-name>
[port <port>]
```

Recovering data from a replication pair

If source replication data becomes inaccessible, it can be *recovered* from the replication pair destination. The source must be empty before recovery can proceed. Recovery can be performed for all replication topologies, except for MTree replication.

Recovery of data from a directory pool, as well as from directory and collection replication pairs, is described in the next sections.

Recovering directory pool data

You can recover data from a directory-based pool, but not from an MTree-based pool.

Procedure

1. Select **More** > **Start Recover**.
2. In the Start Recover dialog, select **Pool** from the **Replication Type** menu.
3. Select the source system hostname from the **System to recover to** menu.
4. Select the destination system hostname from the **System to recover from** menu.
5. Select the context on the destination from which data is recovered.
6. If you want to change any host connection settings, select the **Advanced** tab.
7. Select **OK** to start the recovery.

Recovering collection replication pair data

To successfully recover collection replication pair data, the source file system must be in a pristine state, and the destination context must be fully initialized.

Procedure

1. Select **More** > **Start Recover** to display the Start Recover dialog.

2. Select **Collection** from the **Replication Type** menu.
3. Select the source system host name from the **System to recover to** menu.
4. Select the destination system host name from the **System to recover from** menu.
5. Select the context on the destination from which data is recovered. Only one collection will exist on the destination.
6. To change any host connection settings, select the **Advanced** tab.
7. Select **OK** to start the recovery.

Recovering directory replication pair data

To successfully recover directory replication pair data, the same directory used in the original context must be created (but left empty).

Procedure

1. Select **More > Start Recover** to display the Start Recover dialog.
2. Select **Directory** from the **Replication Type** menu.
3. Select the host name of the *system to which data needs to be restored* from the **System to recover to** menu.
4. Select the host name of the *system that will be the data source* from the **System to recover from** menu.
5. Select the context to restore from the context list.
6. To change any host connection settings, select the **Advanced** tab.
7. Select **OK** to start the recovery.

Aborting a replication pair recovery

If a replication pair recovery fails or must be terminated, you can stop the replication recovery.

Procedure

1. Select the **More** menu, and select **Abort Recover** to display the Abort Recover dialog, which shows the contexts currently performing recovery.
2. Select the checkbox of one or more contexts to abort from the list.
3. Select **OK**.

After you finish

As soon as possible, you should restart recovery on the source.

Resyncing an MTree, directory, or pool replication pair

Resynchronization is the process of recovering (or bringing back into sync) the data between a source and a destination replication pair after a manual break. The replication pair are resynchronized so both endpoints contain the same data. Resynchronization is available for MTree, directory, and pool replication, but not for collection replication.

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.

Procedure

1. Delete the context on both the replication source and replication destination systems.
2. From either the replication source or replication destination system, select **More** > **Start Resync** to display the Start Resync dialog.
3. Select the Replication Type to be resynced: **Directory**, **MTree**, or **Pool**.
4. Select the replication source system host name from the **Source System** menu.
5. Select the replication destination system host name from the **Destination System** menu.
6. Enter the replication source path in the **Source Path** text box.
7. Enter the replication destination path in the **Destination Path** text box.
8. To change any host connection settings, select the **Advanced** tab.
9. Select **OK**.

CLI Equivalent

```
# replication resync Destination
```

Aborting a replication pair resynchronization

If a replication pair resynchronization fails or must be terminated, you can stop the resynchronization.

Procedure

1. From either the replication source or replication destination system, select **More** > **Abort Resync** to display the Abort Resync dialog, which lists all contexts currently performing resynchronization.
2. Select the checkboxes of one or more contexts to abort their resynchronization.
3. Select **OK**.

Converting a directory replication pair to an MTree

When a directory replication pair is converted to an MTree, the directory data is initialized in an MTree, and the directory replication configuration is deleted. The conversion is started with a replication resync that filters all data from the source DD system to the destination DD system.

Here are some estimates for filtering performance:

[MiB = MibiBytes, base-2 equivalent of Megabytes; GiB = GibiBytes, base-2 equivalent of Gigabytes; TiB = TibiBytes, base-2 equivalent of Terabytes]

- Over a T3, 100ms WAN, filtering performance is about 100 MiB/sec, providing a data transfer rate of 100 MiB/sec = 10 seconds/GiB = 8.6 TiB/day.
- Over a gibibit LAN, filtering performance is about 120 MiB/sec, providing a data transfer rate of 120 MiB/sec = 8.3 seconds/GiB = 10.3 TiB/day.

Procedure

1. Create a new MTree on both the source and the destination.
2. Select the directory replication pair in the Summary table.
3. Select **More** > **Convert to MTree** to display the Convert to MTree dialog.
4. Add the new MTree paths to the source and destination text fields.

5. Select **OK**.

A Warning dialog is displayed, indicating the directory data is being initialized in the new MTree, and the old directory replication configuration is being deleted.

6. Select **OK**.

The Convert to MTree Status dialog is displayed, showing the progress of the conversion.

7. Select **Close**.

DD Boost view

The DD Boost view provides configuration and troubleshooting information to NetBackup administrators who have configured DD systems to use DD Boost AIR (Automatic Image Replication) or any DD Boost application that uses managed file replication.

See the *EMC Data Domain Boost for OpenStorage Administration Guide* for DD Boost AIR configuration instructions.

The **File Replication** tab displays:

- Currently Active File Replication:
 - Direction (Out-Going and In-Coming) and the number of files in each.
 - Remaining data to be replicated (pre-compressed value in GiB) and the amount of data already replicated (pre-compressed value in GiB).
 - Total size: The amount of data to be replicated and the already replicated data (pre-compressed value in GiB).
- Most Recent Status: Total file replications and whether completed or failed
 - during the last hour
 - over the last 24 hours
- Remote Systems:
 - Select a replication from the list.
 - Select the time period to be covered from the menu.
 - Select **Show Details** for more information about these remote system files.

The **Storage Unit Associations** tab displays the following information, which you can use for audit purposes or to check the status of DD Boost AIR events used for the storage unit's image replications:

- A list of all storage unit **Associations** known to the system. The source is on the left, and the destination is on the right. This information shows the configuration of AIR on the Data Domain system.
- The **Event Queue** is the pending event list. It shows the local storage unit, the event ID, and the status of the event.

An attempt is made to match both ends of a DD Boost path to form a pair and present this as one pair/record. If the match is impossible, for various reasons, the remote path will be listed as *Unresolved*.

Remote system files

The Show Details button provides information for the selected remote file replication system. File Replications shows starting and ending information, as well as size and data

amount, for the selected remote file replication system. The Performance Graph shows performance over time for the selected remote file replication system.

Table 162 File Replications

Item	Description
Start	Starting point of time period.
End	Ending point of time period.
File Name	Name of specific replication file.
Status	Most recent status (Success, Failure).
Pre-Comp Size (MiB)	Amount of pre-compressed outbound and inbound data, as compared to network throughput or post-compressed data (in MiB).
Network Bytes (MiB)	Amount of network throughput data (in MiB).

Table 163 Performance Graph

Item	Description
Duration	Duration for replication (either 1d, 7d or 30d).
Interval	Interval for replication (either Daily or Weekly).
Pre-Comp Replicated	Amount of pre-compressed outbound and inbound data (in GiB).
Post-Comp Replicated	Amount of post-compressed data (in GiB).
Network Bytes	Amount of network throughput data (in GiB).
Files Succeeded	Number of files that were successfully replicated.
Files Failed	Number of files that failed to be replicated.
Show in new window	Brings up a separate window.
Print	Prints the graph.

Topology view

The Topology view shows how the selected replication pairs are configured in the network.

- The arrow – which is green (normal), yellow (warning), or red (error) – between DD systems represents one or more replication pairs.
- To view details, select a context, which opens the Context Summary dialog, with links to **Show Summary**, **Modify Options**, **Enable/Disable Pair**, **Graph Performance**, and **Delete Pair**.
- Select **Collapse All** to roll-up the Expand All context view and show only the name of the system and the count of destination contexts.
- Select **Expand All** to show all the destination directory and MTree contexts configured on other systems.
- Select **Reset Layout** to return to the default view.
- Select **Print** to open a standard print dialog.

Performance view

The Performance view displays a graph that represents the fluctuation of data during replication. These are aggregated statistics of each replication pair for this DD system.

- **Duration** (x-axis) is 30 days by default.
- **Replication Performance** (y-axis) is in GibiBytes or MebiBytes (the binary equivalents of GigaBytes and MegaBytes).
- **Network In** is the total replication network bytes entering the system (all contexts).
- **Network Out** is the total replication network bytes leaving the system (all contexts).
- For a reading of a specific point in time, hover the cursor over a place on the graph.
- During times of inactivity (when no data is being transferred), the shape of the graph may display a gradually descending line, instead of an expected sharply descending line.

Advanced Settings view

Advanced Settings lets you manage throttle and network settings.

Throttle Settings

- **Temporary Override** – Displays throttle rate if configured, or 0 meaning all replication traffic is stopped.
- **Permanent Schedule** – Displays the time and days of the week on which scheduled throttling occurs.

Network Settings

- **Bandwidth** – Displays the configured data stream rate if bandwidth has been configured, or Unlimited (default) if not. The average data stream to the replication destination is at least 98,304 bits per second (12 KiB).
- **Delay** – Displays the configured network delay setting (in milliseconds) if it has been configured, or None (default) if not.
- **Listen Port** – Displays the configured listen port value if it has been configured, or 2051 (default) if not.

Adding throttle settings

To modify the amount of bandwidth used by a network for replication, you can set a *replication throttle* for replication traffic.

There are three types of replication throttle settings:

- **Scheduled throttle** – The throttle rate is set at a predetermined time or period.
- **Current throttle** – The throttle rate is set until the next scheduled change, or until a system reboot.
- **Override throttle** – The previous two types of throttle are overridden. This persists – even through reboot – until you select **Clear Throttle Override** or issue the `replication throttle reset override` command.

You can also set a default throttle or a throttle for specific destinations, as follows:

- **Default throttle** – When configured, all replication contexts are limited to this throttle, except for those destinations specified by destination throttles (see next item).

- **Destination throttle** – This throttle is used when only a few destinations need to be throttled, or when a destination requires a throttle setting different from the default throttle. When a default throttle already exists, this throttle takes precedence for the destination specified. For example, you can set the default replication throttle to *10 kbps*, but – using a destination throttle – you can set a single collection replication context to *unlimited*.

Note

Currently, you can set and modify destination throttle only by using the command-line interface (CLI); this functionality is not available in the DD System Manager. For documentation on this feature, see the `replication throttle` command in the *EMC Data Domain Operating System Command Reference Guide*. If the DD System Manager detects that you have one or more destination throttles set, you will be given a warning, and you should use the CLI to continue.

Additional notes about replication throttling:

- Throttles are set only at the source. The only throttle that applies to a destination is the **0 Bps (Disabled)** option, which disables all replication traffic.
- The minimum value for a replication throttle is 98,304 bits per second.

Procedure

1. Select **Replication > Advanced Settings > Add Throttle Setting** to display the Add Throttle Setting dialog.
2. Set the days of the week for which throttling is to be active by selecting **Every Day** or by selecting checkbox(es) next to individual day(s).
3. Set the time that throttling is to start with the **Start Time** drop-down selectors for the hour:minute and AM/PM.
4. For **Throttle Rate**:
 - Select **Unlimited** to set no limits.
 - Enter a number in the text box (for example, 20000), and select the rate from the menu (bps, Kbps, Bps, or KBps).
 - Select the **0 Bps (disabled)** option to disable all replication traffic.
5. Select **OK** to set the schedule. The new schedule is shown under **Permanent Schedule**.

Results

Replication runs at the given rate until the next scheduled change, or until a new throttle setting forces a change.

Deleting Throttle Settings

You can delete a single throttle setting or all throttle settings at once.

Procedure

1. Select **Replication > Advanced Settings > Delete Throttle Setting** to display the Delete Throttle Setting dialog.
2. Select the checkbox for the throttle setting to delete, or select the heading checkbox to delete all settings. This list can include settings for the “disabled” state.
3. Select **OK** to remove the setting.
4. In the Delete Throttle Setting Status dialog, select **Close**.

Temporarily overriding a throttle setting

A throttle override temporarily changes a throttle setting. The current setting is listed at the top of the window.

Procedure

1. Select **Replication** > **Advanced Settings** > **Set Throttle Override** to display the Throttle Override dialog.
2. Either set a new throttle override, or clear a previous override.
 - a. To set a new throttle override:
 - Select **Unlimited** to revert to the system-set throttle rate (no throttling performed), or
 - Set the throttling bit and rate in the text box (for example, 20000) and (bps, Kbps, Bps, or KBps), or
 - Select **0 Bps (Disabled)** to set the throttle rate to 0, effectively stopping all replication network traffic.
 - To enforce the change temporarily, select **Clear at next scheduled throttle event**.
 - b. To clear an override previously set, select **Clear Throttle Override**.
3. Select **OK**.

Changing network settings

Using the bandwidth and network-delay settings together, replication calculates the proper TCP (transmission control protocol) buffer size for replication usage. These network settings are global to the DD system and should be set only once per system.

Note the following:

- You can determine the actual bandwidth and the actual network delay values for each server by using the `ping` command.
- The default network parameters in a restorer work well for replication in low latency configurations, such as a local 100Mbps or 1000Mbps Ethernet network, where the latency round-trip time (as measured by the `ping` command) is usually less than 1 millisecond. The defaults also work well for replication over low- to moderate-bandwidth WANs, where the latency may be as high as 50-100 milliseconds. However, for high-bandwidth high-latency networks, some tuning of the network parameters is necessary.
The key number for tuning is the bandwidth-delay number produced by multiplying the bandwidth and round-trip latency of the network. This number is a measure of how much data can be transmitted over the network before any acknowledgments can return from the far end. If the bandwidth-delay number of a replication network is more than 100,000, then replication performance benefits from setting the network parameters in both restorers.

Procedure

1. Select **Replication** > **Advanced Settings** > **Change Network Settings** to display the Network Settings dialog.
2. In the Network Settings area, select **Custom Values**.
3. Enter **Delay** and **Bandwidth** values in the text boxes. The network delay setting is in milliseconds, and bandwidth is in bytes per second.

4. In the Listen Port area, enter a new value in the text box. The default IP Listen Port for a replication destination for receiving data streams from the replication source is 2051. This is a global setting for the DD system.
5. Select **OK**. The new settings appear in the Network Settings table.

Monitoring replication

The DD System Manager provides many ways to track the status of replication – from checking replication pair status, to tracking backup jobs, to checking performance, to tracking a replication process.

Checking replication pair status

Several places in the Replication area of the DD System Manager provide status updates for replication pairs.

Procedure

1. Select **Replication** > **Topology**.
2. Check the colors of the arrows, which provide the status of the context.
3. Select the **Summary** tab.
4. From the **Filter By** drop-down list (under the Create Pair button), select **State**, and select **Error**, **Warning**, or **Normal** from the state menu.

The replication contexts are sorted according to the selection.

Viewing estimated completion time for backup jobs

You can use the Completion Predictor to see the estimated time for when a backup replication job will be completed.

Procedure

1. Select **Replication** > **Summary**.
2. Select a Replication context for which to display Detailed Information.
3. In the Completion Predictor area, select options from the **Source Time** drop-down list for a replication's completion time, and select **Track**.

The estimated time displays, in the Completion Time area, for when a particular backup job will finish its replication to the destination. If the replication is finished, the area shows **Completed**.

Checking replication context performance

To check the performance of a replication context over time, select a Replication context in the Summary view, and select **Performance Graph** in the Detailed Information area.

Tracking status of a replication process

To display the progress of a replication initialization, resynchronization, or recovery operation, use the **Replication** > **Summary** view to check the current state.

CLI Equivalent

```
# replication show config all
```

CTX	Source	Destination
Connection	Host and Port	Enabled

```

-----
-----
1      dir://host2/backup/dir2      dir://host3/backup/dir3
host3.company.com                    Yes
2      dir://host3/backup/dir3      dir://host2/backup/dir2
host3.company.com                    Yes

```

When specifying an IP version, use the following command to check its setting:

```

# replication show config rctx://2
CTX:                2
Source:             mtree://ddbeta1.dallasrdc.com/data/coll/EDM1
Destination:       mtree://ddbeta2.dallasrdc.com/data/coll/EDM_ipv6
Connection Host:   ddbeta2-ipv6.dallasrdc.com
Connection Port:   (default)
Ipversion:         ipv6
Low-bw-optim:     disabled
Encryption:       disabled
Enabled:           yes
Propagate-retention-lock: enabled

```

CHAPTER 14

DD Secure Multitenancy

This chapter includes:

- [Data Domain Secure Multitenancy overview](#) 344
- [Provisioning a Tenant Unit](#) 346
- [Enabling Tenant Self-Service mode](#) 346
- [Data access by protocol](#) 347
- [Data management operations](#) 349

Data Domain Secure Multitenancy overview

Data Domain Secure Multitenancy (SMT) provides secure storage consolidation in *Protection Storage*.

Segregating, isolating, and protecting data of multiple customers – on a single DD system – is the main feature of SMT.

Multiple tenants can simultaneously reside on a single DD system, but the activities of one tenant cannot be detected by another.

Within an enterprise, a tenant may consist of one or more business units or departments on a DD system configured and managed by IT staff.

- For a business unit (BU) use case, the Finance and Human Resources departments of a corporation could share the same DD system, but each department would be unaware of the presence of the other.
- For a service provider (SP) use case, the SP could deploy one or more DD systems to accommodate different Protection Storage services for multiple end-customers.

Both use cases emphasize the segregation of different customer data on the same physical DD system.

Terminology used in SMT

Understanding the terminology used in SMT (Secure Multitenancy) will help you better understand this unique environment.

MTrees

MTrees are logical partitions of the Data Domain file system and offer the highest degree of management granularity, meaning users can perform operations on a specific MTree without affecting the entire file system. MTrees are assigned to Tenant Units and contain that Tenant Unit's individualized settings for managing and monitoring SMT.

Multitenancy

Multitenancy refers to the hosting of an IT infrastructure by an internal IT department, or an external service provider, for more than one consumer/workload (business unit/department/tenant) simultaneously. Data Domain SMT enables *Data Protection-as-a-Service*.

RBAC (role-based access control)

RBAC (role-based access control) offers multiple roles with different privilege levels, which combine to provide the administrative isolation on a multitenant DD system. (The next section will define these roles.)

Storage Unit

A *Storage Unit* is an MTree configured for the DD Boost protocol. Data isolation is achieved by creating a Storage Unit and assigning it to a DD Boost user. The DD Boost protocol permits access only to Storage Units assigned to DD Boost users connected to the DD system.

Tenant

A *tenant* is a consumer (business unit/department/customer) who maintains a persistent presence in a hosted environment.

Tenant self-service

Tenant self-service lets a tenant log in to a DD system to access the Tenant Units assigned to him or her and perform their own administration and reporting for their own environments.

Tenant Unit

A *Tenant Unit* is the partition of a DD system that serves as the unit of administrative isolation between tenants. Tenant Units are secured and logically isolated from each other, which ensures security and isolation of the control path when running multiple tenants simultaneously on the shared infrastructure. Tenant Units can contain one or more *MTrees*, which hold all configuration elements needed in a multitenancy setup. Users, management-groups, notification-groups, and other configuration elements are part of a Tenant Unit.

Data and control path isolation

Control path isolation is achieved by providing the user roles of *tenant-admin* and *tenant-user*. These users are restricted in scope and capability to specific Tenant Units and to a restricted set of operations they can perform on those Tenant Units.

To ensure a logically secure and isolated data path, a system administrator must configure one or more Tenant Unit *MTrees* for each protocol in an SMT environment. Supported protocols include DD Boost, NFS, CIFS, and VTL. Access is strictly regulated by the native access control mechanisms of each protocol.

Understanding RBAC in Secure Multitenancy

In Secure Multitenancy, permission to perform a task depends on the role assigned to a user. DD Management Center uses RBAC (role-based access control) to control these permissions.

All DD Management Center users can:

- View all tenants
- Create, read, update, or delete Tenant Units belonging to any tenant if the user is an administrator on the DD system hosting the Tenant Unit
- Assign and unassign Tenant Units to and from a tenant if the user is an administrator on the DD system hosting the Tenant Unit
- View Tenant Units belonging to any tenant if the user has any assigned role on the DD system hosting the Tenant Unit

To perform more advanced tasks depends on the role of the user, as follows:

admin role

A user with an *admin* role can perform all administrative operations on a DD system. An *admin* can also perform all SMT administrative operations on a DD system, including setting up SMT, assigning SMT user roles, enabling tenant self-service mode, creating a tenant, and so on. In the context of SMT, the *admin* is typically referred to as the *landlord*. In DD OS, the role is known as the *sysadmin*.

To have permission to edit or delete a tenant, you must be both a DD Management Center *admin* and a DD OS *sysadmin* on all DD systems associated with the Tenant Units of that tenant. If the tenant does not have any Tenant Units, you need only to be a DD Management Center *admin* to edit or delete that tenant.

tenant-admin role

A user with a *tenant-admin* role can perform certain tasks only when *tenant self-service* mode is enabled for a specific Tenant Unit. Responsibilities include scheduling and running a backup application for the tenant and monitoring resources and statistics within the assigned Tenant Unit. In addition, *tenant-admins* ensure administrative separation when tenant self-service mode is enabled. In the context of SMT, the *tenant-admin* is usually referred to as the *backup admin*.

tenant-user role

A user with a *tenant-user* role can monitor the performance and usage of SMT components only on Tenant Unit(s) assigned to them and only when tenant self-service is enabled. In addition, *tenant-users* may run the `show` and `list` commands.

none role

A user with a role of *none* is not allowed to perform any operations on a DD system other than changing their password and accessing data using DD Boost. However, after SMT is enabled, the *admin* can select a user with a *none* role from the DD system and assign them an SMT-specific role of *tenant-admin* or *tenant-user*. Then, that user can perform operations on SMT management objects.

management groups

BSPs (backup service providers) can use *management groups* defined in a single, external AD (active directory) or NIS (network information service) to simplify managing user roles on Tenant Units. Each BSP tenant may be a separate, external company and may use a name-service such as AD or NIS.

With SMT management groups, the AD and NIS servers are set up and configured by the *admin* in the same way as SMT local users. The *admin* can ask their AD or NIS administrator to create and populate the group. The *admin* then assigns an SMT role to the entire group. Any user within the group who logs in to the DD system is logged in with the role assigned to the group.

When users leave or join a tenant company, they can be removed or added to the group by the AD or NIS administrator. It is not necessary to modify the RBAC configuration on a DD system when users who are part of the group are added or removed.

Provisioning a Tenant Unit

Launching the configuration wizard begins the initial provisioning procedure for Secure Multitenancy (SMT). During the procedure, the wizard creates and provisions a new Tenant Unit based on Tenant configuration requirements. Information is entered by the administrator, as prompted. After completing the procedure, the administrator proceeds to the next set of tasks, beginning with enabling Tenant Self-Service mode. Following the initial setup, manual procedures and configuration modifications may be performed as required.

Procedure

1. Start SMT.


```
# smt enable
```
2. Verify that SMT is enabled.


```
# smt status
```
3. Launch the SMT configuration wizard.


```
# smt tenant-unit setup
```
4. Follow the configuration prompts.
5. When the procedure concludes, enable Tenant Self-Service mode.

Enabling Tenant Self-Service mode

For administrative separation of duties and delegation of administrative/management tasks to implement Tenant Self-Service, which is required for control path isolation, the system administrator can enable this mode on a Tenant Unit and then assign users to manage the unit in the roles of *tenant-admin* or *tenant-user*. These roles allow users other

than the administrator to perform specific tasks on the Tenant Unit to which they are assigned. In addition to administrative separation, Tenant Self-Service mode helps reduce the management burden on internal IT and service provider staff.

Procedure

1. View Tenant Self-Service mode status for one or all Tenant Units.

```
# smt tenant-unit option show { tenant-unit | all }
```

2. Enable Tenant Self-Service mode on the selected Tenant Unit.

```
# smt tenant-unit option set tenant-unit self-service { enabled | disabled }
```

Data access by protocol

Secure data paths, with protocol-specific access controls, enable security and isolation for Tenant Units. In a Secure Multitenancy (SMT) environment, data access protocol management commands are also enhanced with a Tenant Unit parameter to enable consolidated reporting.

DD systems support multiple data access protocols simultaneously, including DD Boost, NFS, CIFS, and VTL. A DD system can present itself as an application-specific interface, such as a file server offering NFS or CIFS access over the Ethernet, a VTL device, or a DD Boost device.

The native access control mechanisms of each supported protocol ensure that the data paths for each Tenant remain separate and isolated. Such mechanisms include access control lists (ACLs) for CIFS, exports for NFS, DD Boost credentials, and Multi-User Boost credential-aware access control.

Multi-User DD Boost and Storage Units in SMT

When using Multi-User DD Boost with SMT (Secure Multitenancy), user permissions are set by Storage Unit ownership.

Multi-User DD Boost refers to the use of multiple DD Boost user credentials for DD Boost Access Control, in which each user has a separate user name and password.

A *Storage Unit* is an MTree configured for the DD Boost protocol. A user can be associated with, or “own,” one or more Storage Units. Storage Units that are owned by one user cannot be owned by another user. Therefore, only the user owning the Storage Unit can access the Storage Unit for any type of data access, such as backup/restore. The number of DD Boost user names cannot exceed the maximum number of MTrees. (See the “MTrees” chapter in this book for the current maximum number of MTrees for each DD model.)

Each backup application must authenticate using its DD Boost user name and password. After authentication, DD Boost verifies the authenticated credentials to confirm ownership of the Storage Unit. The backup application is granted access to the Storage Unit only if the user credentials presented by the backup application match the user names associated with the Storage Unit. If user credentials and user names do not match, the job fails with a permission error.

Configuring access for CIFS

Common Internet File System (CIFS) is a file-sharing protocol for remote file access. In a Secure Multitenancy (SMT) configuration, backup and restores require client access to

the CIFS shares residing in the MTree of the associated Tenant Unit. Data isolation is achieved using CIFS shares and CIFS ACLs.

Procedure

1. Create an MTree for CIFS.

```
# mtree create mtree-path tenant-unit tenant-unit
```

2. Assign the MTree to the Tenant Unit.

```
# mtree modify mtree-path tenant-unit tenant-unit | none
```

3. Set capacity soft and hard quotas for the MTree.

```
# mtree create mtree-path tenant-unit tenant-unit [quota-soft-limit n{MiB|GiB|TiB|PiB} ] [quota-hard-limit n {MiB|GiB|TiB|PiB}
```

4. Create a CIFS share for *pathname* from the MTree.

```
# cifs share create share path pathname clients clients
```

Configuring NFS access

NFS is a UNIX-based, file-sharing protocol for remote file access. In a Secure Multitenancy (SMT) environment, backup and restores require client access to the NFS exports residing in the MTree of the associated Tenant Unit. Data isolation is achieved using NFS exports and network isolation. NFS determines if an MTree is associated with a network-isolated Tenant Unit. If so, NFS verifies the connection properties associated with the Tenant Unit. Connection properties include the destination IP address and interface or client hostname.

Procedure

1. Create an MTree for NFS.

```
# mtree create mtree-path tenant-unit tenant-unit
```

2. Assign the MTree to the Tenant Unit.

```
# mtree modify mtree-path tenant-unit tenant-unit | none
```

3. Set capacity soft and hard quotas for the MTree.

```
# mtree create mtree-path tenant-unit tenant-unit [quota-soft-limit n{MiB|GiB|TiB|PiB} ] [quota-hard-limit n {MiB|GiB|TiB|PiB}
```

4. Create an NFS export by adding one or more clients to the MTree.

```
# nfs add path client-list
```

Configuring access for VTL

VTL Tenant data isolation is achieved using VTL access groups that create a virtual access path between a host system and the VTL. (The physical Fibre Channel connection between the host system and VTL must already exist.)

Placing tapes in the VTL allows them to be written to, and read by, the backup application on the host system. VTL tapes are created in a VTL pool, which is an MTree. Because VTL pools are MTrees, the pools can be assigned to Tenant Units. This association enables SMT monitoring and reporting.

For example, if a tenant-admin is assigned a Tenant Unit that contains a VTL pool, the tenant-admin can run MTree commands to display read-only information. Commands can run only on the VTL pool assigned to the Tenant Unit.

These commands include:

- `mtree list` to view a list of MTrees in the Tenant Unit

- `mtree show compression` to view statistics on MTree compression
- `mtree show performance` to view statistics on performance

Output from most `list` and `show` commands include statistics that enable service providers to measure space usage and calculate chargeback fees.

VTL operations are unaffected and continue to function normally.

Using VTL NDMP TapeServer

VTL Tenant data isolation is also achieved using NDMP. DD OS implements a NDMP (Network Data Management Protocol) tape server that allows NDMP-capable systems to send backup data to the DD system via a three-way NDMP backup.

The backup data is written to virtual tapes (which are in a pool) by a VTL assigned to the special VTL group *TapeServer*.

Because the backup data is written to tapes in a pool, information in the VTL topic regarding MTrees also applies to the Data Domain NDMP TapeServer.

Data management operations

Secure Multitenancy (SMT) management operations include monitoring Tenant Units and other objects, such as Storage Units and MTrees. For some SMT objects, additional configuration or modification may also be required.

Collecting performance statistics

Each MTree can be measured for performance or “usage” statistics and other real-time information. Historical consumption rates are available for DD Boost Storage Units. Command output lets the tenant-admin collect usage statistics and compression ratios for an MTree associated with a Tenant Unit, or for all MTrees and associated Tenant Units. Output may be filtered to display usage in intervals ranging from minutes to months. Results are passed to the administrator, who uses the statistics as a chargeback metric. A similar method is used to gather usage statistics and compression ratios for Storage Units.

Procedure

1. Collect MTree real-time performance statistics.

```
# mtree show stats
```

2. Collect performance statistics for MTrees associated with a Tenant Unit.

```
# mtree show performance
```

3. Collect compression statistics for MTrees associated with a Tenant Unit.

```
# mtree show compression
```

Modifying quotas

To meet QoS criteria, a system administrator uses DD OS “knobs” to adjust the settings required by the Tenant configuration. For example, the administrator can set “soft” and “hard” quota limits on DD Boost Storage Units. Stream “soft” and “hard” quota limits can be allocated only to DD Boost Storage Units assigned to Tenant Units. After the administrator sets the quotas, the tenant-admin can monitor one or all Tenant Units to ensure no single object exceeds its allocated quotas and deprives others of system resources.

Quotas are set initially when prompted by the configuration wizard, but they can be adjusted or modified later. The example below shows how to modify quotas for DD Boost.

(You can also use `quota capacity` and `quota streams` to deal with capacity and stream quotas and limits.)

Procedure

1. To modify soft and hard quota limits on DD Boost Storage Unit “su33”:

```
ddboost storage-unit modify su33 quota-soft-limit 10 Gib quota-
hard-limit 20 Gib
```

2. To modify stream soft and hard limits on DD Boost Storage Unit “su33”:

```
ddboost storage-unit modify su33 write-stream-soft-limit 20 read-
stream-soft-limit 6 repl -stream-soft-limit 20 combined-stream-
soft-limit 20
```

3. To report physical size for DD Boost Storage Unit “su33”:

```
ddboost storage-unit modify su33 report-physical-size 8 GiB
```

SMT and replication

In case of disaster, user roles dictate how a user can assist in data recovery operations. Several replication types are available in an SMT configuration. (See the *DD Replicator* chapter for more detail on how to perform replication.)

Here are some points to consider regarding user roles:

- The admin can recover MTrees from a replicated copy.
- The tenant-admin can replicate MTrees from one system to another, using DD Boost managed file replication.
- The tenant-admin can recover MTrees from a replicated copy, also by using DD Boost managed file replication.

Collection replication

Collection replication replicates core Tenant Unit configuration information.

MTree replication (NFS/CIFS) using DD Boost managed file replication

MTree replication is supported on MTrees assigned to Tenant Units, using DD Boost managed file replication. During MTree replication, an MTree assigned to a Tenant Unit on one system can be replicated to an MTree assigned to a Tenant Unit on another system.

For backward compatibility, MTree replication from an MTree assigned to a Tenant Unit to an unassigned MTree is supported, but must be configured manually. Manual configuration ensures the destination MTree has the correct settings for the Tenant Unit. Conversely, MTree replication from an unassigned MTree to an MTree assigned to a Tenant Unit is also supported.

DD Boost managed file replication (also with DD Boost AIR)

DD Boost managed file replication is supported between Storage Units, regardless of whether one Storage Unit, or both, are assigned to Tenant Units.

During DD Boost managed file replication, Storage Units are not replicated in total. Instead, certain files within a Storage Unit are selected by the backup application for replication. The files selected in a Storage Unit and assigned to a Tenant Unit on one system can be replicated to a Storage Unit assigned to a Tenant Unit on another system.

For backward compatibility, selected files in a Storage Unit assigned to a Tenant Unit can be replicated to an unassigned Storage Unit. Conversely, selected files in an unassigned Storage Unit can be replicated to a Storage Unit assigned to a Tenant Unit.

DD Boost managed file replication can also be used in DD Boost AIR deployments.

SMT Tenant alerts

A DD system generates *events* when it encounters potential problems with software or hardware. When an event is generated, an *alert* notification is sent immediately via email to members designated in the notification list and to the Data Domain administrator.

SMT alerts are specific to each Tenant Unit and differ from DD system alerts. When Tenant Self-Service mode is enabled, the tenant-admin can choose to receive alerts about the various system objects he or she is associated with and any critical events, such as an unexpected system shutdown. A tenant-admin may only view or modify notification lists to which he or she is associated.

The example below shows a sample alert. Notice that the two event messages at the bottom of the notification are specific to a Multi-Tenant environment (indicated by the word “Tenant”). For the entire list of DD OS and SMT alerts, see the *EMC Data Domain MIB Quick Reference Guide* or the SNMP MIB.

```
EVT-ENVIRONMENT-00021 - Description: The system has been shutdown by
abnormal method; for example, not by one of the following: 1) Via
IPMI chassis control command 2) Via power button 3) Via OS shutdown.
```

```
Action: This alert is expected after loss of AC (main power) event.
If this shutdown is not expected and persists, contact your
contracted support provider or visit us online at https://
my.datadomain.com.
```

```
Tenant description: The system has experienced an unexpected power
loss and has restarted.
```

```
Tenant action: This alert is generated when the system restarts after
a power loss. If this alert repeats, contact your System
Administrator.
```

Managing snapshots

A *snapshot* is a read-only copy of an MTree captured at a specific point in time. A snapshot can be used for many things, for example, as a restore point in case of a system malfunction. The required role for using `snapshot` is `admin` or `tenant-admin`.

To view snapshot information for an MTree or a Tenant Unit:

```
# snapshot list mtree mtree-path | tenant-unit tenant-unit
```

To view a snapshot schedule for an MTree or a Tenant Unit:

```
# snapshot schedule show [name | mtrees mtree-list mtree-list | tenant-
unit tenant-unit]
```

Performing a file system Fast Copy

A Fast Copy operation clones files and directory trees of a source directory to a target directory on a DD system. There are special circumstances regarding Fast Copy with Secure Multitenancy (SMT).

Here are some considerations when performing a file system Fast Copy with Tenant Self-Service mode enabled:

- A tenant-admin can Fast Copy files from one Tenant Unit to another when the tenant-admin is the tenant-admin for both Tenant Units, and the two Tenant Units belong to the same Tenant.
- A tenant-admin can Fast Copy files within the same Tenant Unit.
- A tenant-admin can Fast Copy files within the Tenant Units at source and destination.

To perform a file system Fast Copy:

```
# fileys fastcopy source <src> destination <dest>
```


CHAPTER 15

DD Extended Retention

This chapter includes:

- [DD Extended Retention overview](#)..... 354
- [Supported protocols in DD Extended Retention](#)..... 356
- [Using DD Replicator with DD Extended Retention](#).....356
- [Hardware and licensing for DD Extended Retention](#)..... 357
- [Managing DD Extended Retention](#)..... 361
- [Upgrades and recovery with DD Extended Retention](#).....370

DD Extended Retention overview

EMC Data Domain Extended Retention (DD Extended Retention) provides an internal tiering approach that enables cost-effective, long-term retention of backup data on a DD system. DD Extended Retention lets you leverage DD systems for long-term backup retention and minimize reliance on tape.

Note

DD Extended Retention was formerly known as *Data Domain Archiver*.

Two-Tiered File System

The internal two-tiered file system of a DD Extended Retention-enabled DD system consists of an *active tier* and a *retention tier*. The file system, however, appears as a single entity. Incoming data is first placed in the active tier of the file system. The data (in the form of complete files) is later moved to the retention tier of the file system, as specified by your individual *Data Movement Policy*. For example, the active tier might retain weekly full and daily incremental backups for 90 days, while the retention tier might retain monthly fulls for seven years.

The retention tier is comprised of one or more retention units, each of which may draw storage from one or more shelves.

Note

As of DD OS 5.5.1, only one retention unit per retention tier is allowed. However, systems set up prior to DD OS 5.5.1 may continue to have more than one retention unit, but you will not be allowed to add any more retention units to them. You will also not be able to use *Encryption of Data at Rest* with more than one retention unit.

Transparency of Operation

DD Extended Retention-enabled DD systems support existing backup applications using simultaneous data access methods through NFS and CIFS file service protocols over Ethernet, through VTL for open systems and IBMi, or as a disk-based target using application-specific interfaces, such as DD Boost (for use with EMC Avamar®, EMC NetWorker®, EMC GreenPlum, Symantec OpenStorage, and Oracle RMAN).

DD Extended Retention extends the DD architecture with automatic transparent data movement from the active tier to the retention tier. All of the data in the two tiers is accessible, although there might be a slight delay on initial access to data in the retention tier. The namespace of the system is global and is not affected by data movement. No partitioning of the file system is necessary to take advantage of the two-tiered file system.

Data Movement Policy

The *Data Movement Policy*, which you can customize, is the policy by which files are moved from the active to the retention tier. It is based on the time when the file was last modified. You can set a different policy for each different subset of data, because the policy can be set on a per-MTree basis. Files that may be updated need a policy different from those that never change.

Deduplication within Retention Unit

For fault isolation purposes, deduplication occurs entirely within the retention unit for DD Extended Retention-enabled DD systems. There is no cross-deduplication between active and retention tiers, or between different retention units (if applicable).

Storage Drawn from Each Tier

The concept of tiering extends to the storage level for a DD Extended Retention-enabled DD system. The active tier of the file system draws storage from the active tier of storage. The retention tier of the file system draws storage from the retention tier of storage.

Note

For both active and retention tiers, DD OS 5.2 and later support ES20 and ES30 shelves. Different models cannot be mixed in the same shelf set, and the shelf sets must be balanced according to the configuration rules specified in the *EMC ES30 Shelf Hardware Guide*. You can attach significantly more storage to the same controller, up to a maximum of 56 shelves on a DD990, using DD Extended Retention. The active tier must include storage consisting of at least one shelf.

Data Protection

On a DD Extended Retention-enabled DD system, data is protected with built-in fault isolation features, disaster recovery capability, and DIA (Data Invulnerability Architecture). DIA checks files when they are moved from the active to the retention tier. After data is copied into the retention tier, the container and file system structures are read back and verified. The location of the file is updated, and the space on the active tier is reclaimed after the file is verified to have been correctly written to the retention tier.

When a retention unit is filled up, namespace information and system files are copied into it, so the data in the retention unit may be recovered even when other parts of the system are lost.

Note

Sanitization and some forms of Replication are not supported for DD Extended Retention-enabled DD systems.

Space Reclamation

To reclaim space that has been freed up by data moved to the retention tier, you can use *Space Reclamation* (as of DD OS 5.3), which runs in the background as a low-priority activity. It suspends itself when there are higher priority activities, such as data movement and cleaning.

Encryption of Data at Rest

As of DD OS 5.5.1, you can use the *Encryption of Data at Rest* feature on DD Extended Retention-enabled DD systems, if you have an encryption license. Encryption is not enabled by default.

This is an extension of the encryption capability already available, prior to DD OS 5.5.1, for systems not using DD Extended Retention.

Refer to the *Managing Encryption of Data at Rest* chapter in this guide for complete instructions on setting up and using the encryption feature.

Note

Encryption of Data at Rest is supported only for systems with a single retention unit. As of 5.5.1, DD Extended Retention supports only a single retention unit, so systems set up during, or after, 5.5.1 will have no problem complying with this restriction. However, systems set up prior to 5.5.1 may have more than one retention unit, but they will not work with Encryption of Data at Rest until all but one retention unit has been removed, or data has been moved or migrated to one retention unit.

Supported protocols in DD Extended Retention

DD Extended Retention-enabled DD systems support the protocols NFS, CIFS, and DD Boost. Support for VTL was added in DD OS 5.2, and support for NDMP was added in DD OS 5.3.

Note

For a list of applications supported with DD Boost, see the *DD Boost Compatibility List* on the EMC Online Support site.

When you are using DD Extended Retention, data first lands in the active tier. Files are moved in their entirety into the retention unit in the retention tier, as specified by your Data Movement Policy. All files appear in the same namespace. There is no need to partition data, and you can continue to expand the file system as desired.

All data is visible to all users, and all file system metadata is present in the active tier.

The trade-off in moving data from the active to the retention tier is larger capacity versus slightly slower access time if the unit to be accessed is not currently ready for access.

Using DD Replicator with DD Extended Retention

Some forms of replication are supported on DD Extended Retention-enabled DD systems.

Supported replication types depend on the data to be protected:

- To protect data on a system as a *source*, a DD Extended Retention-enabled DD system supports collection replication, MTree replication, and DD Boost managed file replication.
- To protect data from other systems as a *destination*, a DD Extended Retention-enabled DD system also supports directory replication, as well as collection replication, MTree replication, and DD Boost managed file replication.

Note

Delta (low bandwidth optimization) replication is not supported with DD Extended Retention. You must disable delta replication on all contexts before enabling DD Extended Retention on a DD system.

Collection replication with DD Extended Retention

Collection replication takes place between the corresponding active tier and retention unit of the two DD systems with DD Extended Retention enabled. If the active tier or retention unit at the source fails, the data can be copied from the corresponding unit at the remote site onto a new unit, which is shipped to your site as a replacement unit.

Prerequisites for setting up collection replication include:

- Both the source and destination systems must be configured as DD systems with DD Extended Retention enabled.
- The file system must not be enabled on the destination until the retention unit has been added to it, and replication has been configured.

Directory replication with DD Extended Retention

For directory replication, a DD Extended Retention-enabled DD system serves as a replication target and supports one-to-one and many-to-one topologies from any

supported DD system. However, DD Extended Retention-enabled DD systems do not support bi-directional directory replication and cannot be a *source* of directory replication.

Note

To copy data using directory replication into a DD Extended Retention-enabled DD system, the source must be running DD OS 5.0 or later. Therefore, on systems running DD OS 5.0 or earlier, you must first import data into an intermediate system running DD OS 5.0 or later. For example, replication from a DD OS 4.9 Extended Retention-enabled system could be made into a DD OS 5.2 non-Extended Retention-enabled system. Then, replication could be made from the DD OS 5.2 system into the DD OS 4.9 system.

MTree replication with DD Extended Retention

You can set up MTree replication between two DD Extended Retention-enabled DD systems. Replicated data is first placed in the active tier on the destination system. The Data Movement Policy on the destination system then determines when the replicated data is moved to the retention tier.

Note that MTree replication restrictions and policies vary by DD OS release, as follows:

- As of DD OS 5.1, data can be replicated from a non-DD Extended Retention-enabled system to a DD Extended Retention-enabled system with MTree replication.
- As of DD OS 5.2, data can be protected within an active tier by replicating it to the active tier of a DD Extended Retention-enabled system.
- As of DD OS 5.5, MTree replication is supported from a DD Extended Retention-enabled system to a non-DD Extended Retention-enabled system if both are running DD OS 5.5 or later.
- For DD OS 5.3 and 5.4, if you plan to enable DD Extended Retention, do not set up replication for the /backup MTree on the source machine. (DD OS 5.5 and later do not have this restriction.)

Managed file replication with DD Extended Retention

For DD Extended Retention-enabled DD systems, the supported topologies for DD Boost managed file replication are one-to-one, many-to-one, bi-directional, one-to-many, and cascaded.

Note

For DD Boost 2.3 or later, you can specify how multiple copies are to be made and managed within the backup application.

Hardware and licensing for DD Extended Retention

Certain hardware configurations are required for DD Extended Retention-enabled DD systems. Licensing, specifically separate shelf capacity licenses, is also specific to this feature.

Hardware supported for DD Extended Retention

The hardware requirements for DD Extended Retention-enabled DD systems include memory requirements, shelves, NIC/FC cards, etc.

The following DD systems support DD Extended Retention:

DD860

- 72 GB of RAM
- 1 - NVRAM IO module (1 GB)
- 3 - Quad-port SAS IO modules
- 2 - 1 GbE ports on the motherboard
- 0 to 2 - 1/10 GbE NIC IO cards for external connectivity
- 0 to 2 - Dual-Port FC HBA IO cards for external connectivity
- 0 to 2 - Combined NIC and FC cards
- 1 to 24 - ES20 or ES30 shelves (1 TB or 2 TB disks), not to exceed the system maximum usable capacity of 142 TB

If DD Extended Retention is enabled on a DD860, the maximum usable storage capacity of an active tier is 142 TB. The retention tier can have a maximum usable capacity of 142 TB. The active and retention tiers have a total usable storage capacity of 570 TB.

DD990

- 256 GB of RAM
- 1 - NVRAM IO module (2 GB)
- 4 - Quad-port SAS IO modules
- 2 - 1 GbE ports on the motherboard
- 0 to 4 - 1 GbE NIC IO cards for external connectivity
- 0 to 3 - 10 GbE NIC cards for external connectivity
- 0 to 3 - Dual-Port FC HBA cards for external connectivity
- 0 to 3 - Combined NIC and FC cards, not to exceed three of any one specific IO module
- 1 to 56 - ES20 or ES30 shelves (1, 2, or 3 TB disks), not to exceed the system maximum usable capacity of 570 TB

If DD Extended Retention is enabled on a DD990, the maximum usable storage capacity of the active tier is 570 TB. The retention tier can have a maximum usable capacity of 570 TB. The active and retention tiers have a total usable storage capacity of 1344 TB.

DD4200

- 128 GB of RAM
- 1 - NVRAM IO module (4 GB)
- 4 - Quad-port SAS IO modules
- 1 - 1 GbE port on the motherboard
- 0 to 6 - 1/10 GbE NIC cards for external connectivity
- 0 to 6 - Dual-Port FC HBA cards for external connectivity
- 0 to 6 - Combined NIC and FC cards, not to exceed four of any one specific IO module
- 1 to 16 - ES30 SAS shelves (2 or 3 TB disks), not to exceed the system maximum usable capacity of 192 TB. ES30 SATA shelves (1, 2, or 3 TB disks) are supported for system controller upgrades.

If DD Extended Retention is enabled on a DD4200, the maximum usable storage capacity of the active tier is 192 TB. The retention tier can have a maximum usable capacity of 192 TB. The active and retention tiers have a total usable storage capacity of 576 TB. External connectivity is supported for DD Extended Retention configurations up to 16 shelves.

DD4500

- 192 GB of RAM
- 1 - NVRAM IO module (4 GB)
- 4 - Quad-port SAS IO modules
- 1 - 1 GbE port on the motherboard
- 0 to 6 - 1/10 GbE NIC IO cards for external connectivity
- 0 to 6 - Dual-Port FC HBA cards for external connectivity
- 0 to 5 - Combined NIC and FC cards, not to exceed four of any one specific IO module
- 1 to 20 - ES30 SAS shelves (2 or 3 TB disks), not to exceed the system maximum usable capacity of 285 TB. ES30 SATA shelves (1 TB, 2 TB, or 3 TB) are supported for system controller upgrades.

If DD Extended Retention is enabled on a DD4500, the maximum usable storage capacity of the active tier is 285 TB. The retention tier can have a maximum usable capacity of 285 TB. The active and retention tiers have a total usable storage capacity of 1152 TB. External connectivity is supported for DD Extended Retention configurations up to 32 shelves.

DD7200

- 128 GB of RAM for entry capacity; optional upgrade to 256 GB RAM for expanded capacity
- 1 - NVRAM IO module (4 GB)
- 4 - Quad-port SAS IO modules
- 1 - 1 GbE port on the motherboard
- 0 to 6 - 1/10 GbE NIC cards for external connectivity
- 0 to 6 - Dual-Port FC HBA cards for external connectivity
- 0 to 5 - Combined NIC and FC cards, not to exceed four of any one specific IO module
- 1 to 20 - ES30 SAS shelves (2 or 3 TB disks), not to exceed the system maximum usable capacity of 432 TB. ES30 SATA shelves (1 TB, 2 TB, or 3 TB) are supported for system controller upgrades.

If DD Extended Retention is enabled on a DD7200, the maximum usable storage capacity of the active tier is 432 TB. The retention tier can have a maximum usable capacity of 432 TB. The active and retention tiers have a total usable storage capacity of 1728 TB. External connectivity is supported for DD Extended Retention configurations up to 56 shelves.

DD9500

- 256 GB of RAM for entry capacity; optional upgrade to 512 GB RAM for expanded capacity
- 1 - NVRAM IO module (8 GB)
- 4 - Quad-port SAS IO modules
- 1 - Quad 1 GbE ports on the motherboard
- 0 to 4 - 10 GbE NIC cards for external connectivity
- 0 to 4 - Dual-Port 16 Gbe FC HBA cards for external connectivity
- 1 to 30 - ES30 SAS shelves (2 or 3 TB disks), not to exceed the system maximum usable capacity of 1080 TB

If DD Extended Retention is enabled on a DD9500, the maximum usable storage capacity of the active tier is 1080 TB. The retention tier can have a maximum usable capacity of

1080 TB. The active and retention tiers have a total usable storage capacity of 2160 TB. External connectivity is supported for DD Extended Retention configurations up to 56 shelves.

Licensing for DD Extended Retention

DD Extended Retention is a licensed software option installed on a supported DD system.

A separate shelf capacity license is needed for each storage shelf, for shelves installed in both the active tier and the retention tier. Shelf capacity licenses are specific to either an active or retention tier shelf.

An Expanded-Storage license is required to expand the active tier storage capacity beyond the entry capacity, which varies by Data Domain model. You cannot use the additional storage without first applying the appropriate licenses.

Adding shelf capacity licenses for DD Extended Retention

Every shelf in a DD Extended Retention-enabled DD system must have a separate license.

Procedure

1. Select **System Settings** > **Licenses** tab.
2. Select **Add Licenses**.
3. Enter one or more licenses, one per line, pressing the Enter key after each one. Select **Add** when you are done. If there are any errors, a summary of the added licenses, and those not added because of the error, are listed. Select the erroneous License Key to fix it.

Results

The licenses for the DD system are displayed in two groups:

- Software option licenses, required for options such as DD Extended Retention and DD Boost.
- Shelf Capacity Licenses, which display shelf capacity (in TiB), the shelf model (such as ES30), and the shelf's storage tier (active or retention).

To delete a license, select the license in the Licenses list, and select **Delete Selected Licenses**. If prompted to confirm, read the warning, and select **OK** to proceed.

Configuring storage for DD Extended Retention

Additional storage for DD Extended Retention requires the appropriate license or licenses and enough installed memory on the DD system to support it. Error messages display if more licenses or memory are needed.

Procedure

1. Select **Hardware** > **Storage** tab.
2. In the Overview tab, select **Configure Storage**.
3. In the Configure Storage tab, select the storage to be added from the Available Storage list.
4. Select the appropriate Tier Configuration (or **Active** or **Retention**) from the menu. The active tier is analogous to a standard DD system and should be sized similarly. The maximum amount of storage that can be added to the active tier depends on the DD controller used. The two bars show the portion of licensed capacity used/remaining for each shelf model (ES20 and ES30).

5. Select the checkbox for the Shelf to be added.
6. Select the **Add to Tier** button.
7. Select **OK** to add the storage.
8. To remove an added shelf, select it in the Tier Configuration list, select **Remove from Configuration**, and select **OK**.

Customer-provided infrastructure for DD Extended Retention

Before enabling DD Extended Retention, your environment and setup must meet certain requirements.

- **Specifications, site requirements, rack space, and interconnect cabling:** See the *EMC Data Domain Installation and Setup Guide* for your DD system model.
- **Racking and cabling:** It is recommended that you rack your system with future expansion in mind. All shelves are attached to a single DD system. See the *EMC Data Domain ES20 Expansion Shelf Hardware Guide* for a system consisting of only ES20 shelves, or the *EMC Data Domain ES30 Expansion Shelf Hardware Guide* for a system with ES30 shelves.

Managing DD Extended Retention

To set up and use DD Extended Retention on your DD system, you can use the DD System Manager and/or the DD CLI.

- The DD System Manager, formerly known as the Enterprise Manager, is a graphical user interface (GUI), which is described in this guide.
- The `archive` commands, entered at the DD Command Line Interface (CLI) are described in the *EMC Data Domain Operating System Command Reference Guide*.

The only command not available when you use the DD System Manager is `archive report`.

Enabling DD systems for DD Extended Retention

Before using a DD system for DD Extended Retention, you must have the correct license and the correct file system setup.

Procedure

1. Ensure that the correct license is applied. Select **System Settings** > **Licenses**, and check the Feature Licenses list for Extended Retention.
2. Select **Data Management** > **File System**.
3. Select **More Tasks** > **Enable DD Extended Retention**. This option is available only if the file system has not already been configured for DD Extended Retention. Be aware that after DD Extended Retention has been enabled, it cannot be disabled without disabling the file system.
 - a. If the file system is already enabled (as a non-DD Extended Retention system), you are prompted to disable it. Select **Disable** to do so.
 - b. If prompted to confirm that you want to convert the file system for use by DD Extended Retention, select **OK**.

After a file system is converted into a DD Extended Retention file system, the file system page is refreshed to include information about both tiers, and there is a new tab labeled **Retention Units**.

CLI Equivalent

You can also verify that the Extended Retention license has been installed at the CLI:

```
# license show
## License Key                               Feature
-----
1      DEFA-EFCD-FCDE-CDEF                    Replication
2      EFCD-FCDE-CDEF-DEFA                    VTL
-----
```

If the license is not present, each unit comes with documentation – a quick install card – which will show the licenses that have been purchased. Enter the following command to populate the license key.

Then disable the file system:

```
# fileSYS disable
```

Then add the license:

```
# license add license-code
```

Then enable Extended Retention:

```
# archive enable
```

Creating a two-tiered file system for DD Extended Retention

DD Extended Retention has a two-tiered file system for the active and retention tiers. The DD system must have been enabled for DD Extended Retention before enabling this special file system.

Procedure

1. Select **Data Management** > **File System**.
2. If a file system already exists, disable it.
3. Select **More Tasks** > **Create file system**.
4. Select a retention-capable file system.
5. Select **Next**.
6. You must configure storage before the file system can be created. Select **Configure** in the File System Create dialog.
7. When the Configure Storage Status dialog says the disk enclosures addition has completed, select **Close**.
8. The storage in the active tier is used to create the active file system tier. The storage in the retention tier is used to create a retention unit. Using the File System Create dialog, create an active tier and a retention unit. Select **Next** to confirm.

Note

As of DD OS 5.5.1, only one retention unit per retention tier is allowed. However, systems set up prior to DD OS 5.5.1 may continue to have more than one retention unit, but you will not be allowed to add any more retention units to them.

9. Select the size of the retention unit from the menu.
10. Select **Next**.

A Summary page shows the size of the active and retention tiers in the new file system. You have the option of returning to the previous step to change the allocation size, or of cancelling the procedure.

11. Select **Finish** to enable the file system.

The progress of each step is shown, and a progress bar monitors overall status.

CLI Equivalent

To add additional shelves, use this command once for each enclosure:

```
# storage add tier archive enclosure 5
```

Create an archive unit, and add it to the file system. You will be asked to specify the number of enclosures in the archive unit:

```
# filesystem archive unit add
```

Verify that the archive unit is created and added to the file system:

```
# filesystem archive unit list all
```

Check the file system, as seen by the system:

```
# filesystem show space
Active Tier:
Resource          Size GiB   Used GiB   Avail GiB   Use%   Cleanable GiB
-----
/data: pre-comp   -           0.0         -           -       -
/data: post-comp  21557.8     0.2       21557.7     0%      0.0
/ddvar            132.9       4.0        122.1       3%      -
-----

Archive Tier:
Resource          Size GiB   Used GiB   Avail GiB   Use%   Cleanable GiB
-----
/data: pre-comp   -           8.2         -           -       -
/data: post-comp  43135.7    18.8       43116.9     0%      -
-----

Total:
Resource          Size GiB   Used GiB   Avail GiB   Use%   Cleanable GiB
-----
/data: pre-comp   -           8.2         -           -       -
/data: post-comp  64693.6    19.0       64674.6     0%      0.0
/ddvar            132.9       4.0        122.1       3%      -
-----
* Estimated based on last cleaning of 2010/12/14 16:54:38.
```

File system panel for DD Extended Retention

After you have enabled a DD system for DD Extended Retention, the **Data Management > File System** panel will look slightly different (from a non-DD Extended Retention-enabled system).

- **State** shows that the file system is either enabled or disabled. You can change the state by using the Disable/Enable button immediately to the right.
- **Clean Status** shows the time the last cleaning operation finished, or the current cleaning status if the cleaning operation is currently running. If cleaning can be run, it shows a **Start Cleaning** button. When cleaning is running, the **Start Cleaning** button changes to a **Stop Cleaning** button.
- **Data Movement Status** shows the time the last data movement finished. If data movement can be run, it shows a **Start** button. When data movement is running, the **Start** button changes to a **Stop** button.
- **Space Reclamation Status** shows the amount of space reclaimed after deleting data in the retention tier. If space reclamation can be run, it shows a **Start** button. If it is already running, it shows **Stop** and **Suspend** buttons. If it was running previously and

was suspended, it shows **Stop** and **Resume** buttons. There is also a **More Information** button that will display detailed information about starting and ending times, completion percentage, units reclaimed, space freed, etc.

- Selecting **More Tasks** › **Destroy** lets you delete all data in the file system, including virtual tapes. This can be done only by a system administrator.
- Selecting **More Tasks** › **Fast Copy** lets you clone files and MTrees of a source directory to a destination directory. Note that for DD Extended Retention-enabled systems, fast copy will not move data between the active and retention tiers.
- Selecting **More Tasks** › **Expand Capacity** lets you expand the active or retention tier.

Expanding the active or retention tier

When the file system is enabled, you can expand either the active or the retention tier.

To expand the **active** tier:

Procedure

1. Select **Data Management** › **File System** › **More Tasks** › **Expand Capacity**.
2. In the Expand File System Capacity dialog, select Expand File System Active Tier, then select **Next**.
3. Select **Configure**.
4. In the Configure Storage dialog, make sure that Active Tier is displayed as the Configure selection, and select **OK**.
5. After the configuration completes, you are returned to the Expand File System Capacity dialog. Select **Finish** to complete the active tier expansion.

To expand the **retention** tier:

Procedure

1. Select **Data Management** › **File System** › **More Tasks** › **Expand Capacity**.
2. In the Expand File System Capacity dialog, select Expand File System Retention Tier, then select **Next**.
3. If a retention unit is available, you will see the **Select Retention Unit** dialog. Select the retention unit you want to expand and then **Next**. If a retention unit is not available, you will see the **Create Retention Unit** dialog, and you must create a retention unit before proceeding.

Note

To ensure optimal performance of a DD system with DD Extended Retention enabled, you should always expand the retention tier in at least two-shelf increments. You should also not wait until the retention unit is nearly full before expanding it.

4. Select the size to expand the retention unit, then select **Configure**.
5. After configuration completes, you are returned to the Expand File System Capacity dialog. Select **Finish** to complete the retention tier expansion.

Reclaiming space in the retention tier

You can reclaim space from deleted data in the retention tier by running space reclamation (introduced in DD OS 5.3). Space reclamation also occurs during file system cleaning.

Procedure

1. Select **Data Management** > **File System**. Just above the tabs, **Space Reclamation Status** shows the amount of space reclaimed after deleting data in the retention tier.
2. If space reclamation can be run, it shows a **Start** button. If it is already running, it shows **Stop** and **Suspend** buttons. If it was running previously and was suspended, it shows **Stop** and **Resume** buttons.
3. Select **More Information** for details about the cycle name; start and end times; effective run time; percent completed (if in progress); units reclaimed; space freed on target unit, and total space freed.

CLI Equivalent

To enable space reclamation:

```
# archive space-reclamation start
```

To disable space reclamation:

```
# archive space-reclamation stop
```

To show the status of space reclamation:

```
# archive space-reclamation status-detailed
Space-reclamation will start when 'archive data-movement'
completes.

Previous Cycle:
-----
Start time           : Feb 21 2014 14:17
End time             : Feb 21 2014 14:49
Effective run time   : 0 days, 00:32.
Percent completed    : 00 % (was stopped by user)
Units reclaimed      : None
Space freed on target unit : None
Total space freed    : None
```

File system tabs for DD Extended Retention

After you have enabled a DD system for DD Extended Retention, the **Data Management** > **File System** tabs will also look slightly different (from a non-DD Extended Retention-enabled system), and there will be one additional tab: **Retention Units**

Summary Tab

The Summary tab displays information about disk space usage and compression for both the active and retention tiers.

Space Usage: Shows the total size, amount of space used, and amount of available space and combined totals for active and retention tiers. The amount of cleanable space is shown for the active tier.

Active Tier and Retention Tier: Shows the pre-compression and post-compression values currently used and those written in the last 24 hours. Also shows the global, local, and total compression (reduction percentage) factors.

Retention Units Tab

The Retention Units tab displays the retention unit(s). As of DD OS 5.5.1, only one retention unit per retention tier is allowed. However, systems set up prior to DD OS 5.5.1

may continue to have more than one retention unit, but you will not be allowed to add any more retention units to them.

The following information is displayed: the unit's State (New, Empty, Sealed, Target, or Cleaning), its Status (Disabled, Ready, or Stand-by), its Start Date (when it was moved to the retention tier), and the Unit Size. The unit will be in the cleaning state if space reclamation is running. If the unit has been sealed, meaning no more data can be added, the Sealed Date is provided. Selecting the retention unit's checkbox displays additional information (Size, Used, Available, and Cleanable) in the Detailed Information panel.

There are two buttons: **Delete** (for deleting the unit) and **Expand** (for adding storage to a unit). The unit must be in a new or target state to be expanded.

Configuration Tab

The Configuration Tab lets you configure your system.

Selecting the Options **Edit** button displays the Modify Settings dialog, where you can change Local Compression Type [options are none, lz (the default), gz, and gzfast] and Retention Tier Local Comp(ression) [options are none, lz, gz (the default), and gzfast], as well as enable Report Replica Writable.

Selecting the Clean Schedule **Edit** button displays the Modify Schedule dialog, where you can change the cleaning schedule, as well as the throttle percentage.

Selecting the Data Movement Policy **Edit** button displays the Data Movement Policy dialog, where you can set several parameters. File Age Threshold is a system-wide default that applies to all MTrees for which you have not set a custom default. The minimum value is 14 days. Data Movement Schedule lets you establish how often data movement will be done; the recommended schedule is every two weeks. File System Cleaning lets you elect not to have a system cleaning after data movement; however, it is strongly recommended that you leave this option selected.

File Age Threshold per MTree Link

Selecting the **File Age Threshold per MTree** link will take you from the File System to the MTree area (also accessible by selecting **Data Management > MTree**), where you can set a customized File Age Threshold for each of your MTrees.

Select the MTree, and then select **Edit** next to Data Movement Policy. In the Modify Age Threshold dialog, enter a new value for File Age Threshold, and select **OK**. As of DD OS 5.5.1, the minimum value is 14 days.

Encryption Tab

The Encryption tab lets you enable or disable Encryption of Data at Rest, which is supported only for systems with a single retention unit. As of 5.5.1, DD Extended Retention supports only a single retention unit, so systems set up during, or after, 5.5.1 will have no problem complying with this restriction. However, systems set up prior to 5.5.1 may have more than one retention unit, but they will not work with Encryption of Data at Rest until all but one retention unit has been removed, or data has been moved or migrated to one retention unit.

Space Usage Tab

The Space Usage Tab lets you select one of three chart types [(entire) File System; Active (tier); Archive (tier)] to view space usage over time in MiB. You can also select a duration value (7, 30, 60, or 120 days) at the upper right. The data is presented (color-coded) as pre-compression written (blue), post-compression used (red), and the compression factor (black).

Consumption Tab

The Consumption Tab lets you select one of three chart types [(entire) File System; Active (tier); Archive (tier)] to view the amount of post-compression storage used and the compression ratio over time, which enables you to view consumption trends. You can

also select a duration value (7, 30, 60, or 120 days) at the upper right. The Capacity checkbox lets you choose whether to display the post-compression storage against total system capacity.

Daily Written Tab

The Daily Written Tab lets you select a duration (7, 30, 60, or 120 days) to see the amount of data written per day. The data is presented (color-coded) in both graph and table format as pre-compression written (blue), post-compression used (red), and the compression factor (black).

Expanding a retention unit

To ensure optimal performance, do not wait until a retention unit is nearly full before expanding it, and do not expand it in 1-shelf increments. Storage cannot be moved from the active tier to the retention tier after the file system has been created. Only unused enclosures can be added to the retention tier.

Procedure

1. Select **Data Management** > **File System** > **Retention Units**.
2. Select the retention unit. Note that if it is in the Cleaning state, it cannot be expanded.
3. Select **Expand**.
4. The dialog will show the current retention unit size. Select an estimated size to increase the unit, and select **Next**. If there is insufficient configured storage to expand the unit, a message is displayed. However, after the file system is expanded, you cannot revert it to its original size.
5. To expand the file system using available non-configured storage, select **Configure**.

Deleting a retention unit

If all of the files on a retention unit are no longer needed, deleting them makes the unit available for reuse. You can generate a file location report to make sure that the retention unit is indeed empty, delete the retention unit, and then add it as a new retention unit.

Procedure

1. Disable the file system.
2. Select **Data Management** > **File System** > **Retention Units**.
3. Select the retention unit.
4. Select **Delete**.

Modifying retention tier local compression

You can modify the local compression algorithm for subsequent data movement to the retention tier.

Procedure

1. Select **Data Management** > **File System** > **Configuration**.
2. Select the **Edit** button to the right of **Options**.
3. Select one of the compression options from the Retention Tier Local Compression Type menu, and select **OK**.

The default is gz, which is a zip-style compression that uses the least amount of space for data storage (10% to 20% less than lz on average; however, some data sets achieve much higher compression).

Understanding the Data Movement Policy

A file is moved from the active to the retention tier based on the date it was last modified. For data integrity, the entire file is moved at this time. The *Data Movement Policy* establishes two things: a *File Age Threshold* and a *Data Movement Schedule*. If data has not changed during the period of days set by the File Age Threshold, it is moved from the active to the retention tier on the date established by the Data Movement Schedule.

Note

As of DD OS 5.5.1, the File Age Threshold must be a minimum of 14 days.

You can specify different File Age Thresholds for each defined MTree. An MTree is a subtree within the namespace that is a logical set of data for management purposes. For example, you might place financial data, emails, and engineering data in separate MTrees.

To take advantage of the *space reclamation* feature, introduced in DD OS 5.3, it is recommended that you schedule data movement and file system cleaning on a bi-weekly (every 14 days) basis. By default, cleaning is always run after data movement completes. It is highly recommended that you do not change this default.

Avoid these common sizing errors:

- Setting a Data Movement Policy that is overly aggressive; data will be moved too soon.
- Setting a Data Movement Policy that is too conservative: after the active tier fills up, you will not be able to write data to the system.
- Having an undersized active tier and then setting an overly aggressive Data Movement Policy to compensate.

Be aware of the following caveats related to snapshots and file system cleaning:

- Files in snapshots are not cleaned, even after they have been moved to the retention tier. Space cannot be reclaimed until the snapshots have been deleted.
- It is recommended that you set the File Age Threshold for snapshots to the minimum of 14 days.

Here are two examples of how to set up a Data Movement Policy.

- You could segregate data with different degrees of change into two different MTrees and set the File Age Threshold to move data soon after the data stabilizes. Create MTree A for daily incremental backups and MTree B for weekly fulls. Set the File Age Threshold for MTree A so that its data is *never* moved, but set the File Age Threshold for MTree B to 14 days (the minimum threshold).
- For data that cannot be separated into different MTrees, you could do the following. Suppose the retention period of daily incremental backups is eight weeks, and the retention period of weekly fulls is three years. In this case, it would be best to set the File Age Threshold to nine weeks. If it were set lower, you would be moving daily incremental data that was actually soon to be deleted.

Modifying the Data Movement Policy

You can set different Data Movement Policies for each MTree.

Procedure

1. Select **Data Management** > **File System** > **Configuration**.
2. Select the **Edit** button to the right of **Data Movement Policy**.

3. In the Data Movement Policy dialog, specify the system-wide default File Age Threshold value in number of days. As of DD OS 5.5.1, this value must be greater than or equal to 14 days. This value applies to newly created MTrees and MTrees that have not been assigned a per-MTree age threshold value using the **File Age Threshold per MTree** link (see step 7). When data movement starts, all files that have not been modified for the specified threshold number of days will be moved from the active to the retention tier.
4. Specify a Data Movement Schedule, that is, when data movement should take place; for example, daily, weekly, bi-weekly (every 14 days), monthly, or on the last day of the month. You can also pick a specific day or days, and a time in hours and minutes. It is highly recommended that you schedule data movement and file system cleaning on a bi-weekly (every 14 days) basis, to take advantage of the space reclamation feature (introduced in DD OS 5.3).
5. By default, file system cleaning is always run after data movement completes. It is highly recommended that you leave **Start file system clean after Data Movement** selected.
6. Select OK.
7. Back in the Configuration tab, you can specify age threshold values for individual MTrees by using the **File Age Threshold per MTree** link at the lower right corner.

CLI Equivalent

To set the age threshold:

```
# archive data-movement policy set age-threshold {days|none}
mtreees mtree-list
```

If necessary, to set the *default* age threshold:

```
# archive data-movement policy set default-age-threshold days
```

To verify the age threshold setting:

```
# archive data-movement policy show [mtree mtree-list]
```

To specify the migration schedule:

```
# archive data-movement schedule set days days time time [no-clean]
```

Acceptable schedule values include:

- days sun time 00:00
- days mon,tue time 00:00
- days 2 time 10:00
- days 2,15 time 10:00
- days last time 10:00 - last day of the month

To verify the migration schedule:

```
# archive data-movement schedule show
```

To disable the file cleaning schedule:

Note

The reason for disabling the cleaning schedule is to eliminate a scheduling conflict between cleaning and data movement. At the conclusion of data movement, cleaning will automatically start. If you disable data movement, you should re-enable file system cleaning.

```
# fileys clean set schedule never
```

Starting or stopping data movement on demand

Even when you have a regular Data Movement Policy, you can also start or stop data movement *on demand*.

Procedure

1. Select **Data Management** > **File System**.
2. Select the **Start** button to the right of **Data Movement Status**.
3. The Start Data Movement dialog warns that data is to be moved from the active to the retention tier, as defined by your Data Movement Policy, followed by a file system cleaning. Select **Finish** to start the data movement.

If a file system cleaning happens to already be in progress, data movement will occur after that cleaning completes. However, another cleaning will be automatically started after this on-demand data movement completes, as well.
4. The **Start** button will be replaced by a **Stop** button.
5. At any time, if you want to stop data movement, select **Stop** and select **OK** in the Stop Data Movement dialog to confirm.

Using data movement packing

Data is compacted in the target partition after every file migration (as of DD OS 5.2). By default, this feature, which is called *data movement packing*, is enabled.

When this feature is enabled, the overall compression of the retention tier improves, but there is a slight increase in migration time.

To determine if this feature is enabled, select **Data Management** > **File System** > **Configuration**.

The current value for **Packing data during Retention Tier data movement** can be either Enabled or Disabled. Consult with a system engineer to change this setting.

Upgrades and recovery with DD Extended Retention

The following sections describe how to perform software and hardware upgrades, and how to recover data, for DD Extended Retention-enabled DD systems.

Upgrading to DD OS 5.6 with DD Extended Retention

The upgrade policy for a DD Extended Retention-enabled DD system is the same as for a standard DD system.

Upgrading from up to two major prior releases is supported. For instructions on how to upgrade the DD OS, refer to the upgrade instructions section of the *Release Notes* for the target DD OS version.

When upgrading a DD Extended Retention-enabled DD system to DD OS 5.6, be sure to update existing data movement schedules to bi-weekly (14 days) to take advantage of the space reclamation feature.

DD Extended Retention-enabled DD systems automatically run cleaning after data movement completes; therefore, do not schedule cleaning separately using the DD System Manager or CLI (command line interface).

If the active tier is available, the process upgrades the active tier and the retention unit, and puts the system into a state that the previous upgrade has not been verified to be

complete. This state is cleared by the file system after the file system is enabled and has verified that the retention tier has been upgraded. A subsequent upgrade is not permitted until this state is cleared.

If the active tier is not available, the upgrade process upgrades the system chassis and places it into a state where it is ready to create or accept a file system.

If the retention unit becomes available after the upgrade process has finished, the unit is automatically upgraded when it is plugged into the system, or at the next system start.

Upgrading hardware with DD Extended Retention

You can upgrade a DD Extended Retention-enabled DD system to a later or higher performance DD Extended Retention-enabled DD system. For example, you could replace a DD Extended Retention-enabled DD860 with a DD Extended Retention-enabled DD990

Note

Consult your contracted service provider, and refer to the instructions in the appropriate *System Controller Upgrade Guide*.

This type of upgrade affects DD Extended Retention as follows:

- If the new system has a more recent version of DD OS than the active and retention tiers, the active and retention tiers are upgraded to the new system's version. Otherwise, the new system is upgraded to the version of the active and retention tiers.
- The active and retention tiers that are connected to the new system become owned by the new system.
- If there is an active tier, the registry in the active tier is installed in the new system. Otherwise, the registry in the retention tier with the most recently updated registry is installed in the new system.

Recovering a DD Extended Retention-enabled system

If the active tier, and a subset of the retention units are lost, on a DD Extended Retention-enabled DD system, and there is no replica available, EMC Support may be able to reconstitute any remaining sealed retention units into a new DD system.

A DD Extended Retention-enabled DD system is designed to remain available to service read and write requests when one or more retention units are lost. The file system may not detect that a retention unit is lost until the file system restarts or tries to access data stored in the retention unit. The latter circumstance may trigger a file system restart. After the file system has detected that a retention unit is lost, it returns an error in response to requests for data stored in that unit.

If the lost data cannot be recovered from a replica, EMC Support might be able to clean up the system by deleting the lost retention unit and any files that reside fully or partially in it.

Using replication recovery

The replication recovery procedure for a DD Extended Retention-enabled DD system depends on the replication type

- Collection replication – The new source must be configured as a DD Extended Retention-enabled DD system with the same number (or more) of retention units as the destination. The file system must not be enabled on the new source until the retention units have been added, and replication recovery has been initiated.

Note

If you need to recover only a portion of a system, such as one retention unit, from a collection replica, contact EMC Support.

- MTree replication – See the *MTree Replication* section in the *Working with DD Replicator* chapter.
- DD Boost managed file replication – See the *EMC Data Domain Boost for OpenStorage Administration Guide*.

Recovering from system failures

A DD Extended Retention-enabled DD system is equipped with tools to address failures in different parts of the system.

Procedure

1. Restore the connection between the system controller and the storage. If the system controller is lost, replace it with a new system controller.
2. If there is loss of data and a replica is available, try to recover the data from the replica. If a replica is not available, limit any loss of data by leveraging the fault isolation features of DD Extended Retention through EMC Support.

CHAPTER 16

DD Retention Lock

This chapter includes:

- [DD Retention Lock overview](#) 374
- [Supported data access protocols](#) 376
- [Enabling DD Retention Lock on an MTree](#) 377
- [Client-Side Retention Lock file control](#) 380
- [System behavior with DD Retention Lock](#) 385

DD Retention Lock overview

When data is locked on an MTree that is enabled with the DD Retention Lock software option, DD Retention Lock helps ensure that data integrity is maintained. Any data that is locked cannot be overwritten, modified, or deleted for a user-defined retention period of up to 70 years.

There are two DD Retention Lock editions:

- *EMC Data Domain Retention Lock Governance Edition* retains the functionality of Data Domain Retention Lock software prior to DD OS 5.2. You can use Data Domain Retention Lock Governance to define retention policies on data that is to be retained for a specific period of time to meet internal IT governance policies implemented by the system administrator.
- *EMC Data Domain Retention Lock Compliance Edition* enables you to meet the strictest data permanence requirements of regulatory standards, such as those of SEC 17a-4(f). The full list of regulatory standards includes:
 - CFTC Rule 1.31b
 - FDA 21 CFR Part 11
 - Sarbanes-Oxley Act
 - IRS 98025 and 97-22
 - ISO Standard 15489-1
 - MoREQ2010

For certification information, see *Compliance Assessments - Summary and Conclusions – EMC Data Domain Retention Lock Compliance Edition* at:

<https://www.emc.com/collateral/analyst-reports/cohasset-dd-retention-lock-assoc-comp-assess-summ-ar.pdf>

(Login is required.)

Compliance with these standards ensures that files locked on a Data Domain system using Data Domain Retention Lock Compliance Edition software cannot be altered or destroyed before the retention period expires. Data Domain Retention Lock Compliance Edition requires a security officer for implementation of policies. An audit log file is accessible by the administrator or security officer.

Each edition requires a separate, add-on license, and either or both can be used on a single Data Domain system.

The retention-locking protocol is the same for both the DD Retention Lock Governance and Compliance Editions. The differences in use stem from the system behavior for the DD Retention Lock Compliance Edition, since it places strict restrictions to meet compliance requirements. For an overview, see the *EMC Data Domain Retention Lock Software – A Detailed Review* (a white paper) available at:

<https://www.emc.com/collateral/hardware/white-papers/h10666-data-domain-retention-lock-wp.pdf>

(Login is required.)

The DD Retention Lock Governance Edition does not require a security officer and provides a higher degree of flexibility for archive data retention on Data Domain systems.

For archive compliance storage requirements, SEC rules require that a separate copy of retention-locked data must be stored with the same retention requirements as the original. Retention-locked files can be replicated using DD Replicator software to another

Data Domain system. If a retention-locked file is replicated, it remains retention locked on the destination system, with the same level of protection as the source file.

The topics that follow provide additional information on the DD Retention Lock software option.

DD Retention Lock protocol

Only files that are explicitly committed to be retention-locked files are retention locked on the Data Domain system. Files are committed to be retention-locked files through client-side file commands issued while DD Retention Lock Governance or Compliance is enabled on the MTree containing the files.

Note

Linux, Unix, and Windows client environments are supported.

Files that are written to shares or exports that are not committed to be retained (even if DD Retention Lock Governance or Compliance is enabled on the MTree containing the files) can be modified or deleted at any time.

Retention locking prevents any modification or deletion of files under retention from occurring directly from CIFS shares or NFS exports during the retention period specified by a client-side *atime* update command. Some archive applications and backup applications can issue this command when appropriately configured. Applications or utilities that do not issue this command cannot lock files using DD Retention Lock.

Retention-locked files are always protected from modification and premature deletion, even if retention locking is subsequently disabled or if the retention-lock license is no longer valid.

You cannot rename or delete non-empty folders or directories within an MTree that is retention-lock enabled. However, you can rename or delete empty folders or directories and create new ones.

The retention period of a retention-locked file can be extended (but not reduced) by updating the file's *atime*.

For both DD Retention Lock Governance and Compliance, once the retention period for a file expires, the file can be deleted using a client-side command, script, or application. However, the file cannot be modified even after the retention period for the file expires. The Data Domain system never automatically deletes a file when its retention period expires.

DD Retention Lock flow

The general flow of activities with DD Retention Lock.

1. Enable MTrees for DD Retention Lock Governance or Compliance retention locking using the DD System Manager or DD OS commands issued from the system console.
2. Commit files to be retention locked on the Data Domain system using client-side commands issued by an appropriately configured archiving or backup application, manually, or via scripts.

Note

Windows clients may need to download utility programs for DD OS compatibility.

3. Optionally, extend file retention times using client-side commands.
4. Optionally, delete files with expired retention periods using client-side commands.

Supported data access protocols

DD Retention Lock is compatible with industry-standard, NAS-based Write-Once-Read-Many (WORM) protocols, and integration is qualified with archive applications such as Symantec Enterprise Vault, EMC SourceOne, EMC Cloud Tiering Appliance, EMC DiskXtender, and so on. Customers using backup applications such as CommVault can also develop custom scripts to use the EMC Data Domain Retention Lock software option.

To check whether an archive application is tested and certified for DD Retention Lock, refer to the *EMC Data Domain Archive Application Compatibility Guide*.

The protocol support of DD Retention Lock software is as follows:

- NFS is supported with both DD Retention Lock Governance and Compliance.
- CIFS is supported with both DD Retention Lock Governance and Compliance.
- VTL is supported with DD Retention Lock Governance, but not with DD Retention Lock Compliance.

Virtual tapes, here referred to as *tapes*, are represented as files on the Data Domain file system.

- When you create a storage pool, a collection of tapes that map to a directory on the file system, you are creating an MTree, unless you specifically select to create the older style directory pool (for backward compatibility). You can also convert storage pools created prior to DD OS 5.3 to MTrees. These MTrees can be retention locked and replicated.
- You can retention-lock one or more tapes using the `vtl tape modify` command, described in the *EMC Data Domain Operating System Command Reference Guide*.
The `mtree retention-lock revert path` command can be used to revert the retention-locked state of tapes locked with the `vtl tape modify` command. After the tape is unlocked, updates can be made to it. The unlocked state won't be visible via the DD System Manager or CLI until the VTL service is disabled then enabled; however, updates will be applied to the unlocked tape. This capability is only for the DD Retention Lock Governance Edition.
- The retention time for tapes can be displayed using the `vtl tape show` command with the `time-display retention` argument.
- You can retention-lock an individual tape using the DD System Manager.

- DD Boost is supported with both DD Retention Lock Governance and Compliance. If client-side scripts are used to retention-lock backup files or backup images, and if a backup application (Symantec NetBackup, for example) is also used on the system via DD Boost, be aware that the backup application may not share the context of the client-side scripts. Thus, when a backup application attempts to expire or delete files that were retention locked via the client-side scripts, space is not released on the EMC Data Domain system.

Data Domain recommends that administrators change their retention period policy to align with the retention lock time. This applies to all the backup applications that are integrated with DD Boost: Avamar, Symantec NetBackup, Symantec Backup Exec, EMC NetWorker, and so on.

Enabling DD Retention Lock on an MTree

Only files within DD Retention Lock Governance or Compliance enabled MTrees can be retention-locked.

MTrees enabled for DD Retention Lock Compliance cannot be converted to DD Retention Lock Governance MTrees and vice versa.

The procedures that follow show how to enable MTrees for either DD Retention Lock Governance or DD Retention Lock Compliance.

Enabling DD Retention Lock Governance on an MTree

Complete the steps below to add a DD Retention Lock Governance license to a system, and then enable DD Retention Lock Governance on one or more MTrees.

Procedure

1. Log in to the DD System Manager.

The DD System Manager window appears with `DD Network` in the Navigation Panel.

2. Select a Data Domain system.

In the Navigation Panel, expand `DD Network` and select a system.

3. Add the DD Retention Lock Governance license, if it is not present.

Click the `System Settings > Licenses` tabs. If `RETENTION-LOCK-GOVERNANCE` is not listed, add it as follows:

- a. In the Licensed Features Panel, click **Add**. The Add License Key dialog box appears.
- b. In the License Key text box, enter the license key.

Note

License keys are case-insensitive. Include the hyphens when entering keys.

- c. Click **OK**. The added license appears in the license list.
4. Select an MTree for retention locking.

Click the `Data Management > MTree` tab, then the checkbox for the MTree you want to use for retention locking. (You can also create an empty MTree and add files to it later.)

5. Display information for the MTree you selected.

Click the MTree Summary tab.

6. Bring up the MTree's Modify Retention Lock dialog box.

Scroll down to Retention Lock and click **Edit** in the Retention Lock area. The dialog box appears.

7. Enable DD Retention Lock Governance on the MTree and change the default minimum and maximum retention lock periods for the MTree, if necessary.

Perform the following actions in the Modify Retention Lock dialog box:

- a. Click the **Enable** checkbox to enable DD Retention Lock Governance on the MTree.
- b. To change the minimum or maximum retention period for the MTree, go to the Retention Period Panel and modify the minimum or maximum time period:

Type a number for the interval in the text box (for example, **5** or **14**).

From the drop-down list, select an interval (minutes, hours, days, years).

Note

Specifying a minimum retention period of less than 12 hours, or a maximum retention period longer than 70 years, results in an error.

- c. Click **OK** to save your settings.

After you close the Modify Retention Lock dialog box, updated MTree information appears.

8. Check retention lock information for the MTree.

Note the following retention lock fields:

- Top:
 - The Status field indicates the Read/Write access for the MTree, the type of retention locking on the MTree, and whether retention locking is enabled or disabled.
- Bottom:
 - The Status field indicates whether retention locking is enabled for the MTree.
 - The Retention Period field indicates minimum and maximum retention periods for the MTree. The retention period specified for a file in the MTree must be equal to or greater than the minimum retention period and equal to or less than the maximum retention period.
 - The UUID field is a unique identification number generated for the MTree.

Repeat steps 4–8 to enable additional MTrees.

Note

To check retention lock configuration settings for any MTree, select the MTree in the Navigation Panel, then click the Summary tab.

9. When you are finished, exit the DD System Manager.

After you finish

Retention-lock files in a retention-lock-enabled MTree.

Enabling DD Retention Lock Compliance on an MTree

Add a DD Retention Lock Compliance license to a system, set up a system administrator and one or more security officers, configure and enable the system to use DD Retention Lock Compliance software, and then enable DD Retention Lock Compliance on one or more MTrees.

Note

For DD OS 5.5, the DD System Manager does not support DD Retention Lock Compliance.

Procedure

1. Add the DD Retention Lock Compliance license on the system, if it is not present.
 - a. First, check whether the license is already installed.


```
license show
```
 - b. If the RETENTION-LOCK-COMPLIANCE feature is not displayed, install the license.


```
license add license-key
```

Note

License keys are case-insensitive. Include the hyphens when entering keys.

2. Set up and one or more security officer user accounts according to Role-Base Access Control (RBAC) rules.
 - a. In the sysadmin role, add a security officer account.


```
user add userrole security
```
 - b. Enable the security officer authorization.


```
authorization policy set security-officer enabled
```
3. Configure and enable the system to use DD Retention Lock Compliance.

Note

Enabling DD Retention Lock compliance enforces many restrictions on low-level access to system functions used during troubleshooting. Once enabled, the only way to disable DD Retention Lock Compliance is to completely initialize and reload the system, which will result in destroying all data on the system.

- a. Configure the system to use DD Retention Lock Compliance.


```
system retention-lock compliance configure
```

The system automatically reboots.
- b. After the reboot process is complete, enable DD Retention Lock Compliance on the system.


```
system retention-lock compliance enable
```
4. Enable compliance on an MTree that will contain retention-locked files.


```
mtree retention-lock enable mode compliance mtree mtree-path
```

Note

Compliance cannot be enabled on /backup, DD Boost storage unit MTrees, or pool MTrees.

5. To change the default minimum and maximum retention lock periods for a compliance-enabled MTree, enter the following commands with security officer authorization.

```
mtree retention-lock set min-retention-period period mtree
mtree-path
mtree retention-lock set max-retention-period period mtree
mtree-path
```

Note

The retention *period* is specified in the format [number] [unit]. For example: 1 min, 1 hr, 1 day, 1 mo, or 1 year. Specifying a minimum retention period of less than 12 hours, or a maximum retention period longer than 70 years, results in an error.

Repeat steps 4 and 5 to enable additional MTrees.

After you finish

Retention lock files in a retention-lock-enabled MTree.

Client-Side Retention Lock file control

This section describes the DD Retention Lock client command interface for locking files stored on EMC Data Domain systems. Client commands are the same for DD Retention Lock Governance and Compliance. Linux, Unix, and Windows client environments are supported; however, Windows clients may need to download utility programs with commands to lock files.

Note

If your application already supports industry-standard WORM, writing a WORM file to a DD Retention Lock Governance or Compliance enabled MTree will lock the file on the Data Domain system. The retention time in the application should agree with the DD Retention Lock settings. You do not need to use the commands described in this section. To check whether an application is tested and certified for the DD Retention Lock, refer to the *EMC Data Domain Archive Application Compatibility Guide*.

Note

Some client machines using NFS, but running a legacy OS, cannot set retention time later than 2038. The NFS protocol doesn't impose the 2038 limit and allows to specifying times until 2106. Further, DD OS doesn't impose the 2038 limit.

Client-side commands are used to manage the retention locking of individual files. These commands apply to all retention-lock-capable Data Domain systems and must be issued in addition to the setup and configuration of the DD Retention Lock software on the Data Domain system.

Required Tools for Windows Clients

You need the `touch.exe` command to perform retention-locking from a Windows-based client.

To obtain this command, download and install utilities for Linux/Unix-based applications according to your Windows version. These utilities are best recommendations from EMC and should be used per customer environment.

- For Windows 8, Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003, and Windows XP:
<http://sourceforge.net/projects/unxutils/files/latest>
- For Windows Server 2008, Windows Vista Enterprise, Windows Vista Enterprise 64-bit edition, Windows Vista SP1, Windows Vista Ultimate, and Windows Vista Ultimate 64-bit edition:
<http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=23754>
- For Windows Server 2003 SP1 and Windows Server 2003 R2:
<http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=20983>

Note

The `touch` command for Windows may have a different format than the Linux examples in this chapter.

Follow the installation instructions provided and set the search path as needed on the client machine.

Client Access to Data Domain System Files

After an MTree is enabled for DD Retention Lock Governance or Compliance, you can:

- Create a CIFS share based on the MTree. This CIFS share can be used on a client machine.
- Create an NFS mount for the MTree and access its files from the NFS mount point on a client machine.

Note

The commands listed in this section are to be used only on the client. They cannot be issued through the DD System Manager or CLI. Command syntax may vary slightly, depending on the utility you are using.

The topics that follow describe how to manage client-side retention lock file control.

Setting Retention Locking on a file

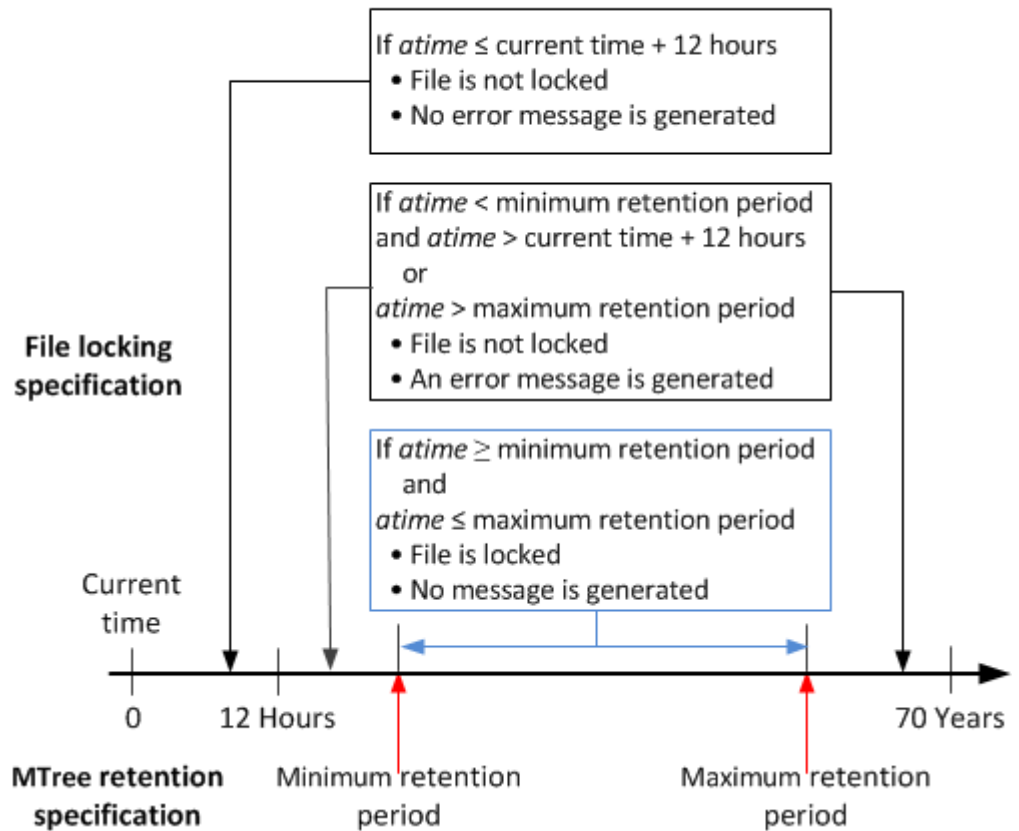
To perform retention locking on a file, change the last access time (*atime*) of the file to the desired retention time of the file, that is, the time when the file can be deleted.

This action is usually performed using the archive application, and all the archive applications that are qualified on Data Domain systems today (per the *EMC Data Domain Archive Application Compatibility Guide*) follow the basic locking protocol outlined here.

The future *atime* you specify must respect the minimum and maximum retention periods of the file's MTree (as offsets from the current time), as shown in the next figure.

Figure 16 Valid and invalid *atime*s for retention locking files

For DD Retention Lock Governance and Compliance



Note

Some client machines using NFS, but running a legacy OS, cannot set retention time later than 2038. The NFS protocol doesn't impose the 2038 limit and allows to specifying times until 2106. Further, DD OS doesn't impose the 2038 limit.

Errors are permission-denied errors (referred to as EACCESS, a standard POSIX error). These are returned to the script or archive application setting the *atime*.

Note

A file must be completely written to the Data Domain system before it is committed to be a retention-locked file.

The following command can be used on clients to set the *atime*:

```
touch -a -t [atime] [filename]
```

The format of *atime* is:

```
[ [YY]YY ] MMDDhhmm[.ss]
```

For example, suppose the current date and time is 1 p.m. on January 18, 2012 (that is, 201201181300), and the minimum retention period is 12 hours. Adding the minimum retention period of 12 hours to that date and time results in a value of 201201190100. Therefore, if the *atime* for a file is set to a value greater than 201201190100, that file becomes retention locked.

The following command:

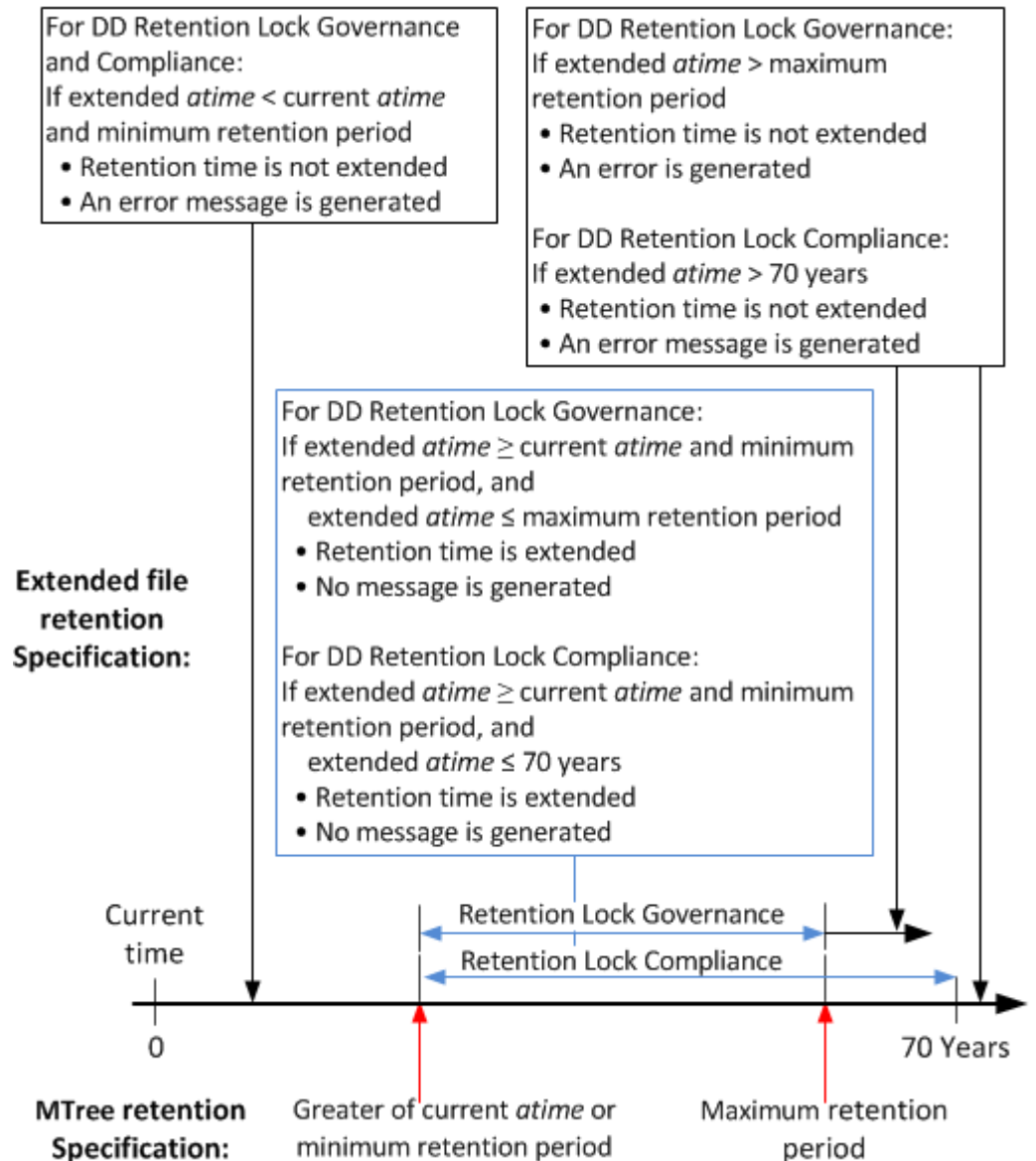
```
ClientOS# touch -a -t 201412312230 SavedData.dat
```

will lock file `SavedData.dat` until 10:30 p.m. December 31, 2014.

Extending Retention Locking on a file

To extend the retention time of a retention-locked file, set the file's `atime` to a value greater than the file's current `atime` but less than the maximum retention period of the file's MTree (as an offset from the current time), as shown in the next figure.

Figure 17 Valid and invalid `atimes` for extending retention locking on files



For example, changing the `atime` from 201412312230 to 202012121230 using the following command:

```
ClientOS# touch -a -t 202012121230 SavedData.dat
```

will cause the file to be locked until 12:30 p.m. December 12, 2020.

Note

Some client machines using NFS, but running a very old OS, cannot set retention time later than 2038. The NFS protocol doesn't impose the 2038 limit and allows to specifying times until 2106. Further, DD OS doesn't impose the 2038 limit.

Errors are permission-denied errors (referred to as EACCESS, a standard POSIX error). These are returned to the script or archive application setting the *atime*.

Identifying a Retention-Locked file

The *atime* value for a retention-locked file is its retention time. To determine whether a file is retention locked, try to set the *atime* of the file to a value earlier than its current *atime*. This action will fail with a permission-denied error if and only if the file is a retention-locked file.

First, list the current *atime* value, and then execute the `touch` command with an earlier *atime* using these commands:

```
ls -l --time=atime [filename]
touch -a -t [atime] [filename]
```

The following example shows the command sequence:

```
ClientOS# ls -l --time=atime SavedData.dat
202012121230
ClientOS# touch -a -t 202012111230 SavedData.dat
```

If the *atime* of `SavedData.dat` is 202012121230 (12:30 p.m. December 12, 2020) and the `touch` command specifies an earlier *atime*, 202012111230 (12:30 p.m. December 11, 2020), the `touch` command fails, indicating that `SavedData.dat` is retention-locked.

Note

The `--time=atime` option is not supported in all versions of Unix.

Specifying a directory and touching only those files

Use the command line to create a root directory containing the files for which access times will change.

In this routine, *root directory to start from* contains the files on which you want to change access times using this client system command:

```
find [root directory to start from] -exec touch -a -t
[expiration time] {} \;
```

For example:

```
ClientOS# find [/backup/data1/] -exec touch -a -t 202012121230 {} \;
```

Reading a list of files and touching only those files

In this routine, *name of file list* is the name of a text file that contains the names of the files on which you want to change access times. Each line contains the name of one file.

Here is the client system command syntax:

```
touch -a -t [expiration time] 'cat [name of file list]'
```

For example:


```
ClientOS# touch -a -t 202012121230 `cat /backup/data1/filelist.txt`
```

Deleting or expiring a file

Delete or expire a file with an expired retention lock using a client application, or delete a file using a standard file-delete command.

Expiring a file using an application makes the file inaccessible to the application. The file may or may not actually be removed from the Data Domain system by the expiration operation. If it is not removed, the application often provides a separate delete operation.

Note

If the retention period of the retention-locked file has not expired, the delete operation results in a permission-denied error.

You must have the appropriate access rights to delete the file, independent of the DD Retention Lock software.

Using `ctime` or `mtime` on Retention-Locked files

ctime is the last-metadata-change time of a file.

`ctime`

ctime gets set to the current time when any of the follow events occur:

- A non-retention-locked file is retention locked.
- The retention time of a retention-locked file is extended.
- A retention-locked file is reverted.

`mtime`

mtime is the last-modified time of a file. It changes only when the contents of the file change. So, the *mtime* of a retention-locked file cannot change.

System behavior with DD Retention Lock

System behavior topics are discussed separately for DD Retention Lock Governance and DD Retention Lock Compliance in the sections that follow.

DD Retention Lock governance

Certain DD OS commands behave differently when using DD Retention Lock Governance. The following sections describe the differences for each.

Replication

Collection replication, MTree replication, and directory replication replicate the locked or unlocked state of files.

Files that are governance retention locked on the source are governance retention locked on the destination and have the same level of protection. For replication, both the source and destination systems must have a DD Retention Lock Governance license installed.

Replication is supported between systems that are:

- Running the same major DD OS version (for example, both systems are running DD OS 5.5.x.x).

- Running DD OS versions within the next two consecutive higher or lower major releases (for example, 5.3.x.x to 5.5.x.x or 5.5.x.x to 5.3.x.x). Cross-release replication is supported only for directory and MTree replication.

Note

MTree replication is not supported for DD OS 5.0 and earlier.

Be aware that:

- Collection replication and MTree replication replicate the minimum and maximum retention periods configured on MTrees to the destination system.
- Directory replication does not replicate the minimum and maximum retention periods to the destination system.

The procedure for configuring and using collection, MTree, and directory replication is the same as for Data Domain systems that do not have a DD Retention Lock Governance license.

Replication Resync

The `replication resync destination` command tries to bring the destination into sync with the source when the MTree or directory replication context is broken between destination and source systems. This command cannot be used with collection replication. Note that:

- 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.

Fastcopy

When the `filesystems fastcopy [retention-lock] source src destination dest` command is run on a system with a DD Retention Lock Governance enabled MTree, the command preserves the retention lock attribute during the fastcopy operation.

Note

If the destination MTree is not retention lock enabled, the retention-lock file attribute is not preserved.

Filesys destroy

Effects of the `filesystems destroy` command when it is run on a system with a DD Retention Lock Governance enabled MTree.

- All data is destroyed, including retention-locked data.
 - All `filesystems` options are returned to their defaults. This means that retention locking is disabled and the minimum and maximum retention periods are set back to their default values on the newly created file system.
-

Note

This command is not allowed if DD Retention Lock Compliance is enabled on the system.

MTree delete

When the `mtree delete mtree-path` command attempts to delete a DD Retention Lock Governance enabled (or previously enabled) MTree that currently contains data, the command returns an error.

Note

The behavior of `mtree delete` is similar to a command to delete a directory—an MTree with retention lock enabled (or previously enabled) can be deleted only if the MTree is empty.

DD Retention Lock compliance

Certain DD OS commands behave differently when using DD Retention Lock Compliance. The following sections describe the differences for each.

Replication

An MTree enabled with Retention Lock Compliance can be replicated via MTree and collection replication only. Directory replication is not supported.

MTree and collection replication replicate the locked or unlocked state of files. Files that are compliance retention locked on the source are compliance retention locked on the destination and have the same level of protection. Minimum and maximum retention periods configured on MTrees are replicated to the destination system.

To perform collection replication, the same security officer user must be present on both the source and destination systems before starting replication to the destination system and afterward for the lifetime of the source/replica pair.

Replication Resync

The `replication resync destination` command can be used with MTree replication, but not with collection replication.

- If the destination MTree contains retention-locked files that do not exist on the source, then resync will fail.
- Both source and destination MTrees must be enabled for Retention Lock Compliance, or resync will fail.

Replication procedures

The topics in this section describe MTree and collection replication procedures supported for Retention Lock Compliance.

Note

For full descriptions of the commands referenced in the following topics, see the *EMC Data Domain Operating System Command Reference Guide*.

Replicating an MTree: One-to-one topology

Replicate a Retention Lock Compliance enabled MTree from a source system to a destination system.

Before you begin

Enable DD Retention Lock on an MTree and configure client-side retention lock file control before replication.

Procedure

1. Until instructed otherwise, perform the following steps on the destination system only.
2. Add the DD Retention Lock Compliance license on the system, if it is not present.
 - a. First, check whether the license is already installed.

```
license show
```

- b. If the RETENTION-LOCK-COMPLIANCE feature is not displayed, install the license.

```
license add license-key
```

Note

License keys are case-insensitive. Include the hyphens when entering keys.

3. Set up and one or more security officer user accounts according to Role-Based Access Control (RBAC) rules.
 - a. In the sysadmin role, add a security officer account.

```
user add user role security
```

- b. Enable the security officer authorization.

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

4. Configure and enable the system to use DD Retention Lock Compliance.
-

Note

Enabling DD Retention Lock compliance enforces many restrictions on low-level access to system functions used during troubleshooting. Once enabled, the only way to disable DD Retention Lock Compliance is to completely initialize and reload the system, which will result in destroying all data on the system.

- a. Configure the system to use DD Retention Lock Compliance.

```
system retention-lock compliance configure
```

The system automatically reboots.

- b. After the reboot process is complete, enable DD Retention Lock Compliance on the system.

```
system retention-lock compliance enable
```

5. Create a replication context.

```
replication add source mtree://source-system-name/data/coll/mtree-name destination mtree://destination-system-name/data/coll/mtree-name
```

6. Perform the following steps on the source system only.

7. Create a replication context.

```
replication add source mtree://source-system-name/data/coll/mtree-name destination mtree://destination-system-name/data/coll/mtree-name
```

8. Initialize the replication context.

```
replication initialize mtree://destination-system-name/data/
coll/mtree-name
```

9. Confirm that replication is complete.

```
replication status mtree://destination-system-name/data/
coll/mtree-name detailed
```

This command reports 0 pre-compressed bytes remaining when replication is finished.

Replicating an MTree: One-to-many topology

Replicate a Retention Lock Compliance enabled MTree from a source system to multiple destination systems.

Before you begin

Enable DD Retention Lock compliance on an MTree and configure client-side retention lock file control before replication.

Procedure

1. Until instructed otherwise, perform the following steps on the destination system only.
2. Add the DD Retention Lock Compliance license on the system, if it is not present.

- a. First, check whether the license is already installed.

```
license show
```

- b. If the RETENTION-LOCK-COMPLIANCE feature is not displayed, install the license.

```
license add license-key
```

Note

License keys are case-insensitive. Include the hyphens when entering keys.

3. Set up and one or more security officer user accounts according to Role-Base Access Control (RBAC) rules.

- a. In the sysadmin role, add a security officer account.

```
user add userrole security
```

- b. Enable the security officer authorization.

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

4. Configure and enable the system to use DD Retention Lock Compliance.

Note

Enabling DD Retention Lock compliance enforces many restrictions on low-level access to system functions used during troubleshooting. Once enabled, the only way to disable DD Retention Lock Compliance is to completely initialize and reload the system, which will result in destroying all data on the system.

- a. Configure the system to use DD Retention Lock Compliance.

```
system retention-lock compliance configure
```

The system automatically reboots.

- b. After the reboot process is complete, enable DD Retention Lock Compliance on the system.

```
system retention-lock compliance enable
```

5. Create a replication context.

```
replication add source mtree://source-system-name/data/coll/  
mtree-name destination mtree://destination-system-name/data/  
coll/mtree-name
```

6. Perform the following steps on the source system only.

7. Create a replication context for each destination system.

```
replication add source mtree://source-system-name/data/coll/  
mtree-name destination mtree://destination-system-name/data/  
coll/mtree-name
```

8. Initialize the replication context for each destination system MTree.

```
replication initialize mtree://destination-system-name/data/  
coll/mtree-name
```

9. Confirm that replication is complete for each destination system.

```
replication status mtree://destination-system-name/data/  
coll/mtree-name detailed
```

This command reports 0 pre-compressed bytes remaining when replication is finished.

Adding Retention Lock Compliance protection to an existing MTree replication pair

Add DD Retention Lock Compliance protection to an existing MTree replication pair that is not enabled for retention locking.

Procedure

1. Until instructed otherwise, perform the following steps on both the source and destination systems.

2. Log in to the DD System Manager.

The DD System Manager window appears with DD Network in the Navigation Panel.

3. Select a Data Domain system.

In the Navigation Panel, expand DD Network and select a system.

4. Add the DD Retention Lock Governance license, if it is not present.

Click the System Settings › Licenses tabs. If RETENTION-LOCK-GOVERNANCE is not listed, add it as follows:

- a. In the Licensed Features Panel, click **Add**. The Add License Key dialog box appears.
- b. In the License Key text box, enter the license key.

Note

License keys are case-insensitive. Include the hyphens when entering keys.

- c. Click **OK**. The added license appears in the license list.

5. Break the current MTree context on the replication pair.

```
replication break mtree://destination-system-name/data/coll/
mtree-name
```

6. Create the new replication context.

```
replication add source mtree://source-system-name/data/coll/
mtree-name destination mtree://destination-system-name/data/
coll/mtree-name
```

7. Perform the following steps on the source system only.

8. Select an MTree for retention locking.

Click the Data Management > MTree tab, then the checkbox for the MTree you want to use for retention locking. (You can also create an empty MTree and add files to it later.)

9. Display information for the MTree you selected.

Click the MTree Summary tab.

10. Lock files in the compliance-enabled MTree.

11. Ensure that both source and destination (replica) MTrees are the same.

```
replication resync mtree://destination-system-name/data/
coll/mtree-name
```

12. Check the progress of resync.

```
replication watch mtree://destination-system-name/data/coll/
mtree-name
```

13. Confirm that replication is complete.

```
replication status mtree://destination-system-name/data/
coll/mtree-name detailed
```

This command reports 0 pre-compressed bytes remaining when replication is finished.

Converting a collection replication pair to MTree replication pairs

A procedure for customers who used collection replication under DD Retention Lock Compliance in DD OS 5.2 and want to upgrade compliance-enabled MTrees in the collection replication pair to MTree replication pairs.

Procedure

1. On the source system only:

a. Create a snapshot for each Retention Lock Compliance enabled MTree.

```
snapshot create snapshot-name /data/coll/mtree-name
```

b. Synchronize the collection replication pair.

```
replication sync col://destination-system-name
```

c. Confirm that replication is complete.

```
replication status col://destination-system-name detailed
```

This command reports 0 pre-compressed bytes remaining when replication is finished.

d. View snapshot information for each Retention Lock Compliance enabled MTree.

```
snapshot list mtree /data/coll/mtree-name
```

Note the snapshot names for use later.

2. On the destination system only:

- a. Confirm that the replication is complete.

```
replication status mtree://destination-system-name/data/
coll/mtree-name detailed
```

This command reports 0 pre-compressed bytes remaining when replication is finished.

- b. View each MTree snapshot replicated to the destination system.

```
snapshot list mtree /data/coll/mtree-name
```

- c. Ensure that all Retention Lock Compliance MTree snapshots have been replicated by comparing the snapshot names generated here with those generated on the source system.

```
snapshot list mtree /data/coll/mtree-name
```

3. On the both the source and destinations systems:

- a. Disable the file system.

```
fileSYS disable
```

- b. Break the collection replication context.

```
replication break col://destination-system-name
```

- c. Enable the file system. (Security officer authorization may be required.)

```
fileSYS enable
```

- d. Add a replication context for each Retention Lock Compliance enabled MTree.

```
replication add source mtree://source-system-name/data/
coll/mtree-name destination mtree://destination-system-
name/data/coll/mtree-name
```

Note

Source and destination MTree names must be the same.

4. On the source system only:

- a. Ensure that both source and destination MTrees are the same.

```
replication resync mtree://destination-system-name
```

- b. Check the progress of resync.

```
replication watch destination
```

- c. Confirm that replication is complete.

```
replication status mtree://destination-system-name/data/
coll/mtree-name detailed
```

This command reports 0 pre-compressed bytes remaining when replication is finished.

Performing collection replication

Replicate `/data/col1` from a compliance-enabled source system to a compliance-enabled destination system.

Note

For collection replication the same security officer account must be used on both the source and destination systems.

Procedure

1. Until instructed to do differently, perform the following steps on the source system only.
 2. Log in to the DD System Manager.

The DD System Manager window appears with `DD Network` in the Navigation Panel.
 3. Select a Data Domain system.

In the Navigation Panel, expand `DD Network` and select a system.
 4. Add the DD Retention Lock Governance license, if it is not present.

Click the `System Settings > Licenses` tabs. If `RETENTION-LOCK-GOVERNANCE` is not listed, add it as follows:

 - a. In the Licensed Features Panel, click **Add**. The Add License Key dialog box appears.
 - b. In the License Key text box, enter the license key.
-

Note

License keys are case-insensitive. Include the hyphens when entering keys.

- c. Click **OK**. The added license appears in the license list.
5. Create the replication context.


```
replication add source col://source-system-name destination
col://destination-system-name
```
6. Until instructed to do differently, perform the following steps on the destination system only.
7. Destroy the file system.


```
filesys destroy
```
8. Log in to the DD System Manager.

The DD System Manager window appears with `DD Network` in the Navigation Panel.
9. Select a Data Domain system.

In the Navigation Panel, expand `DD Network` and select a system.
10. Create a file system, but do not enable it.


```
filesys create
```
11. Create the replication context.

```
replication add source col://source-system-name destination
col://destination-system-name
```

12. Configure and enable the system to use DD Retention Lock Compliance.

```
system retention-lock compliance configure
```

(The system automatically reboots and executes the `system retention-lock compliance enable` command.)

13. Perform the following steps on the source system only.

14. Initialize the replication context.

```
replication initialize source col://source-system-name
destination col://destination-system-name
```

15. Confirm that replication is complete.

```
replication status col://destination-system-name detailed
```

This command reports 0 pre-compressed bytes remaining when replication is finished.

Adding Retention Lock Compliance protection to an existing collection replication pair

Add DD Retention Lock Compliance protection to a collection replication pair that was created without DD Retention Lock Compliance enabled on the source and destination systems.

Procedure

1. Until instructed otherwise, perform the following steps on both the source and destination systems.

2. Disable the replication.

```
replication disable col://destination-system-name
```

3. Log in to the DD System Manager.

The DD System Manager window appears with `DD Network` in the Navigation Panel.

4. Select a Data Domain system.

In the Navigation Panel, expand `DD Network` and select a system.

5. Until instructed otherwise, perform the following steps on the source system.

6. Configure and enable the system to use DD Retention Lock Compliance.

```
system retention-lock compliance configure
```

(The system automatically reboots by executing the `system retention-lock compliance enable` command.)

7. Enable the replication context.

```
replication enable col://destination-system-name
```

8. Until instructed otherwise, perform the following steps on the destination system.

9. Configure and enable the system to use DD Retention Lock Compliance.

```
system retention-lock compliance configure
```

(The system automatically reboots by executing the `system retention-lock compliance enable` command.)

10. Enable the replication context.

```
replication enable col://destination-system-name
```

Fastcopy

When the `fileSYS fastcopy [retention-lock] source src destination dest` command is run on a system with a DD Retention Lock Compliance enabled MTree, the command preserves the retention lock attribute during the fastcopy operation.

Note

If the destination MTree is not retention lock enabled, the retention-lock file attribute is not preserved.

CLI usage

Considerations for a Data Domain system with DD Retention Lock Compliance.

- Commands that break compliance cannot be run. The following commands are disallowed:
 - `fileSYS archive unit del archive-unit`
 - `fileSYS destroy`
 - `mtree delete mtree-path`
 - `mtree retention-lock reset {min-retention-period period | max-retention-period period} mtree mtree-path`
 - `mtree retention-lock disable mtree mtree-path`
 - `mtree retention-lock revert`
 - `user reset`
- The following command requires security officer authorization if the license being deleted is for DD Retention Lock Compliance:
 - `license del license-feature [license-feature ...] | license-code [license-code ...]`
- The following commands require security officer authorization if DD Retention Lock Compliance is enabled on an MTree specified in the command:
 - `mtree retention-lock set {min-retention-period period | max-retention-period period} mtree mtree-path`
 - `mtree rename mtree-path new-mtree-path`
- The following commands require security officer authorization if DD Retention Lock Compliance is enabled on the system:
 - `alerts notify-list reset`
 - `config set timezone zonename`
 - `config reset timezone`
 - `cifs set authentication active-directory realm { [dc1 [dc2 ...]]`
 - `license reset`
 - `ntp add timeserver time server list`
 - `ntp del timeserver time server list`
 - `ntp disable`

- `ntp enable`
- `ntp reset`
- `ntp reset timeservers`
- `replication break {destination | all}`
- `replication disable {destination | all}`
- `system set date MMDDhhmm[[CC]YY]`

System clock

DD Retention Lock Compliance implements an internal security clock to prevent malicious tampering with the system clock.

The security clock closely monitors and records the system clock. If there is an accumulated two-week skew within a year between the security clock and the system clock, the Data Domain file system (DDFS) is disabled and can be resumed only by a security officer.

Finding the System Clock Skew

You can run the DD OS command `system retention-lock compliance status` (security officer authorization required) to get system and security clock information, including the last recorded security clock value, and the accumulated system clock variance. This value is updated every 10 minutes.

Removing the system clock skew

Clock skew is updated every time the security clock records a new value for the system clock. After 1 year, it is reset to 0.

At any time, you can run the DD OS command `system set date MMDDhhmm[[CC]YY]` to set the time of the system clock (security officer authorization required). If the clock skew becomes larger than the preset value (2 weeks), the file system is disabled. Complete these steps to restart the file system and remove the skew between security and system clocks.

Procedure

1. At the system console, enable the file system.

```
fileSYS enable
```

2. At the prompt, confirm that you want to quit the `fileSYS enable` command and check whether the system date is right.

3. Display the system date.

```
system show date
```

4. If the system date is not correct, set the correct date (security officer authorization is required) and confirm it.

```
system set date MMDDhhmm[[CC]YY]
system show date
```

5. Enable the file system again.

```
fileSYS enable
```

6. At the prompt, continue to the enabling procedure.

7. A security officer prompt appears. Complete the security officer authorization to start the file system. The security clock will automatically be updated to the current system date.

CHAPTER 17

DD Encryption

This chapter includes:

- [DD encryption overview](#) 398
- [Configuring encryption](#) 399
- [About key management](#) 400
- [Key manager setup](#) 405
- [Changing key managers after setup](#) 407
- [Checking settings for encryption of data at rest](#) 409
- [Enabling and disabling encryption of data at rest](#) 409
- [Locking and unlocking the file system](#) 410

DD encryption overview

Data encryption protects user data if the Data Domain system is stolen or if the physical storage media is lost during transit, and it eliminates accidental exposure of a failed drive if it is replaced.

When data enters the Data Domain system using any of the supported protocols (NFS, CIFS, VTL, DD Boost, and NDMP Tape Server), the stream is segmented, fingerprinted, and de-duplicated (global compression). It is then grouped into multi-segment compression regions, locally compressed, and encrypted before being stored to disk.

Once enabled, the Encryption at Rest feature encrypts all data entering the Data Domain system. You cannot enable encryption at a more granular level.

CAUTION

Data that has been stored before the encryption feature is enabled does not automatically get encrypted. To protect all of the data on the system, be sure to enable the option to encrypt existing data when you configure encryption.

Additional Notes:

As of DD OS 5.5.1.0, Encryption of Data at Rest is supported for DD Extended Retention-enabled systems with a single retention unit. As of 5.5.1.0, DD Extended Retention supports only a single retention unit, so systems set up during, or after, 5.5.1.0 will have no problem complying with this restriction. However, systems set up prior to 5.5.1.0 may have more than one retention unit, but they will not work with Encryption of Data at Rest until all but one retention unit has been removed, or data has been moved or migrated to one retention unit.

The `filesys encryption apply-changes` command applies any encryption configuration changes to all data present in the file system during the next cleaning cycle. For more information about this command, see the *EMC Data Domain Operating System Command Reference Guide*.

Encryption of Data at Rest supports all of the currently supported backup applications described in the Backup Compatibility Guides available through EMC Online Support at <http://support.emc.com>.

Data Domain Replicator software can be used with the encryption option, enabling encrypted data to be replicated using collection, directory, MTree, or application-specific managed file replication with the various topologies. Each replication form works uniquely with encryption and offers the same level of security. For more information, see the section on using encryption of data at rest with replication.

Files locked using the Data Domain Retention Lock software options can be stored, encrypted, and replicated.

The autosupport feature includes information about the state of encryption on the Data Domain system:

- Whether or not encryption is enabled
- The Key Manager in effect and which keys are used
- The encryption algorithm that is configured
- The state of the file system

Configuring encryption

This procedure includes configuring a key manager.

If the Encryption Status on the **Data Management > File System > Encryption** tab shows Not Configured, click **Configure** to set up encryption on the Data Domain system.

Provide the following information:

- Algorithm
 - Select an encryption algorithm from the drop-down list or accept the default AES 256-bit (CBC).
The AES 256-bit Galois/Counter Mode (GCM) is the most secure algorithm but it is significantly slower than the Cipher Block Chaining (CBC) mode.
 - Determine what data is to be encrypted: existing and new or only new. Existing data will be encrypted during the first cleaning cycle after the file system is restarted. Encryption of existing data can take longer than a standard file system cleaning operation.
- Key Manager (select one of the two)
 - Embedded Key Manager
By default, the Data Domain Embedded Key Manager is in effect after you restart the file system unless you configure the RSA DPM Key Manager.

You can enable or disable key rotation. If enabled, enter a rotation interval between 1-12 months.
 - RSA DPM Key Manager

Note

See the section about key management for an explanation about how the Embedded Key Manager and the RSA DPM Key Manager work.

Note

The RSA DPM Key Manager requires setup on both an RSA DPM server and on the Data Domain system. Follow the instructions in the RSA DPM key manager encryption setup section before selecting the RSA DPM Key Manager in the Data Domain interface. You can enable encryption using the Embedded Key Manager before configuring the RSA DPM Key Manager. You can then switch to the RSA DPM Key Manager after performing an RSA DPM key manager encryption setup and following the procedure described in the changing key managers after setup section.

Table 164 Configuring RSA Key Manager

- Enter the name or the IP address of the Key Manager server.
 - Choose the key class that the Data Domain system will use to generate the key from the menu.
 - Enter the port number (443 is the default).
 - Select whether the imported host certificate is FIPS compliant. The default mode is enabled.
-

The Summary shows your selected configuration values. Review them for correctness. To change a value, click Back to navigate to the page where it was entered and modify it.

A system restart is necessary to enable encryption. To apply the new configuration, select the option to restart the file system.

Note

Applications may experience an interruption while the file system is restarted.

About key management

Encryption keys determine the output of the cryptographic algorithm. They are protected by a passphrase, which encrypts the encryption key before it is stored in multiple locations on disk. The passphrase is user generated and requires both an administrator and a security officer to change it.

A key manager controls the generation, distribution, and lifecycle management of multiple encryption keys. A Data Domain system can use either the Embedded Key Manager or the RSA Data Protection Manager (DPM) Key Manager. Only one can be in effect at a time. When encryption is enabled on a Data Domain system, the Embedded Key Manager is in effect by default. If you configure the RSA DPM Key Manager, it replaces the Embedded Key Manager and remains in effect until you disable it. A file system restart is required for a new key manager to be operational.

Both key managers provide multiple keys, although the system uses only one key at a time to encrypt data coming into a Data Domain system. If the RSA DPM Key Manager is configured and enabled, the Data Domain systems use keys provided by the RSA DPM Key Manager Server. If the same DPM Key Manager manages multiple Data Domain systems, all systems will have the same active key (if they are using the same key class) when the systems are synced and the Data Domain file system has been restarted. The Embedded Key Manager generates its keys internally.

Both key managers rotate keys and support a maximum of 254 keys. The Embedded Key Manager allows you to specify how many months a key is in effect before being replaced (after the file system is restarted). The RSA DPM Key Manager rotates keys on a regular basis, depending on the key class. The Embedded Key Manager key rotation is managed on the Data Domain system. The DPM Key Manager key rotation is managed on the RSA DPM Key Manager server.

The section covers the following major topics.

Rectifying lost or corrupted keys

Create a file that contains all of your system's current encryption keys. Your support provider can use this file to import keys back to your system should they become lost or corrupted. It is recommended that you create an export file on a regular basis.

You are prompted for the Security Officer's credential to export the keys. For additional key file protection, you can use a passphrase that differs from the one used in a Data Domain system. After exporting, it is recommended that you save the key file in a secure file server accessible only by authorized users. You must remember the passphrase used for the key file. If the passphrase is lost or forgotten, the Data Domain system cannot import and restore the keys. Enter:

```
# filesys encryption keys export
```


Key manager support

Both Key Managers support all DD OS file system protocols.

Replication

When configuring Data Domain systems for directory MTree replication, configure each Data Domain system separately. The two systems can use either the same or a different key class, and the same or different key managers.

For collection replication configuration, the Data Domain system must be configured on the source. After a replication break, the original replica Data Domain system has to be configured for the Key Manager. If not, the Data Domain system continues to use the latest known key.

Working with the RSA DPM Key Manager

If the RSA DPM Key Manager is configured and enabled, the Data Domain systems use keys provided by the RSA DPM Key Manager Server. If the same DPM Key Manager manages multiple Data Domain systems, all systems will have the same active key (if they are using the same key class) when the systems are synced and the Data Domain file system has been restarted. Key rotation is managed on the RSA DPM Key Manager server.

If the RSA DPM Key Manager is configured and enabled, the Data Domain systems use keys provided by the RSA DPM Key Manager Server. If the same DPM Key Manager manages multiple Data Domain systems, all systems will have the same active key (if they are using the same key class) when the systems are synced and the Data Domain file system has been restarted. Key rotation is managed on the RSA DPM Key Manager server.

Encryption Key States

One Activated-RW key is always in effect. If the active key is compromised, the RSA DPM Key Manager provides a new key. When the Data Domain system detects the new key, it issues an alert for the administrator to restart the file system.

Expired keys become read only for the existing data on the Data Domain system, and a new active key is applied to all new data that is ingested. When a key is compromised, the existing data is re-encrypted using the new encryption key after a file system cleaning is run. If the maximum number of keys is reached, unused keys must be deleted to make room for new keys.

To view information about the encryption keys that are on Data Domain system, open the DD System Manager and go to the **Data Management** > **File System** > **Encryption** tab. Keys are listed by ID number in the **Encryption Keys** section of the Encryption tab. The following information is given for each key: when a key was created, how long it is valid, its type (RSA DPM or Data Domain), its state (see DPM Encryption Key States Supported by Data Domain), and its post-compression size. If the system is licensed for Extended Retention, the following fields are also displayed:

Active Size (post comp)

The amount of physical space on the active tier encrypted with the key.

Retention Size (post comp)

The amount of physical space on the retention tier encrypted with the key.

Click on a Key MUID and the system displays the following information for the key in the Key Details dialog: Tier/Unit (example: Active, Retention-unit-2), creation date, valid until date, state (see DPM Encryption Key States Supported by Data Domain), and post compression size. Click Close to close the dialog.

Table 165 DPM encryption key states supported by Data Domain

State	Definition
Pending-Activated	The key has just been created. After a file system restart, the key becomes Activated-RW.
Activated-RW and Activated-RO	Both Activated-RW and Activated-RO read the data encrypted with their keys, respectively. Activated-RW is the latest activated key.
De-Activated	A key becomes deactivated when the current time exceeds the validity period. The key is used for reading.
Compromised	The key can only decrypt. After all of the data encrypted with the compromised key is re-encrypted, the state changes to Destroyed Compromised. The keys are re-encrypted when a file system cleaning is run. You can delete a Destroyed Compromised key, if necessary.
Marked-For-Destroy	You have marked the key as destroyed for the data to be re-encrypted.
Destroyed	<p>After re-encrypting all data encrypted with this key, the DD OS changes it from Marked-For-Destroy to Destroyed. Also, when the key that is destroyed is compromised, it becomes Compromised-Destroyed. You can delete keys that are Destroyed and Compromised-Destroyed.</p> <hr/> <p>Note</p> <p>A key is not destroyed in the Data Domain system until a cleaning operation is run and completed.</p> <hr/>

Keeping keys in sync with the RSA DPM key manager

An automatic key sync is performed every day at midnight. A manual key sync is required only if you cannot wait for the scheduled sync. Whenever new keys are synced on the Data Domain system, an alert is generated. This alert is cleared after the Data Domain file system is restarted.

After the RSA DPM Key Manager Server generates new keys, click the **Sync** button to have them display in the Encryption Key list on the Data Domain System Manager's Encryption tab.

Note

A file system restart is necessary if keys have changed since the last sync.

Procedure

1. Using the DD System Manager, select the Data Domain system you are working with in the Navigation panel.

Note

Always perform DD System Manager functions on the system you have selected in the Navigation panel.

2. Click **Data Management > File System** and then select the Encryption tab.
3. In the Encryption Keys section, select the **RSA DPM** key, and click **Sync**.

Destroying a key (RSA DPM key manager)

Destroy a key if you do not want any data to be encrypted with it. This procedure requires security officer credentials.

Note

For information about the security officer, see the sections regarding creating local users and enabling security authorization.

To change an RSA DPM key to a state in which it can be destroyed:

Procedure

1. Deactivate the key on the RSA DPM Server.
2. Restart the file system for the key to be deactivated on the Data Domain system.
3. Using the DD System Manager, navigate to the **Data Management > File System > Encryption** tabs.
4. In the Encryption Keys section, select the key in the list to be destroyed.
5. Click **Destroy....**

The system displays the Destroy dialog that includes the tier and state for the key.

6. Enter your security officer user name and password.
 7. Confirm that you want to destroy the key by clicking **Destroy**.
-

Note

After a file system clean has run, the key state will change to Destroyed.

Deleting a key

You can delete Key Manager keys that are in the Destroyed or Compromised-Destroyed states. However, you only need to delete a key when the number of keys has reached the maximum 254 limit. This procedure requires security officer credentials.

Note

To reach the Destroyed state, the Destroying a Key procedure (for either the Embedded Key Manager or the RSA DPM Key Manager) must be performed on the key and a system cleaning must be run.

Procedure

1. Using the DD System Manager, navigate to the **Data Management > File System > Encryption** tabs.
2. In the Encryption Keys section, select the key or keys in the list to be deleted.
3. Click **Delete....**

The system displays the key to be deleted, and the tier and state for the key.

4. Enter your security officer user name and password.
5. Confirm that you want to delete the key or keys by clicking **Delete**.

Working with the Embedded Key Manager

When the Embedded Key Manager is selected, the Data Domain System creates its own keys.

After the key rotation policy is configured, a new key is automatically created at the next rotation. An alert informs you of the creation of a new key. You must perform a file system restart to activate the new key and deactivate the old key. You can disable the key rotation policy by clicking the disable button associated with the Embedded Key Manager Key's rotation status.

Creating a key (Embedded Key Manager)

Create an encryption key for the Embedded Key Manager.

Procedure

1. Using the DD System Manager, navigate to the **Data Management > File System > Encryption** tabs.
2. In the Encryption Keys section, click the **Create...** button.
3. Enter your security officer user name and password.
4. Select **Restart the filesystem now** if you want to restart the file system.

A new Data Domain key will be created. After the file system is restarted, the previous key will become deactivated and the new key will become activated.

5. Click **Create**.

Destroying a key (Embedded Key Manager)

Destroy an encryption key for the Embedded Key Manager.

Procedure

1. Using the DD System Manager, navigate to the **Data Management > File System > Encryption** tabs.
2. In the Encryption Keys section, select the key in the list to be destroyed.
3. Click **Destroy....**

The system displays the Destroy dialog that includes the tier and state for the key.

4. Enter your security officer user name and password.
5. Confirm that you want to destroy the key by clicking **Destroy**.

Note

After a file system clean has run, the key state changes to Destroyed.

How the cleaning operation works

Encryption affects the performance of cleaning operations when data encrypted with the Compromised or Marked-For-Destroyed keys is re-keyed using the Activated-RW key.

At the end of the cleaning operation, there will be no data that is encrypted with the Compromised or Marked-For-Destroyed keys. Also, any data written by the cleaning operation is encrypted with the Activated-RW key.

Key manager setup

Follow the instructions for the type of key manager you are using.

RSA DPM Key Manager encryption setup

RSA DPM Key Manager must be set up on both the RSA DPM Server and on the Data Domain system.

Performing this setup on the RSA DPM server

The main steps for setting up the RSA DPM Server (using its graphical user interface).

Note

See the latest version of the *RSA Data Protection Manager Server Administrator's Guide* for more information about each step of this procedure.

Algorithm and cipher mode settings set on the RSA DPM Key Manager Server are ignored by the Data Domain system. Configure these settings on the Data Domain system.

Procedure

1. Create an identity for the Data Domain system using the X509 certificate. A secure channel is created based on this certificate.
2. Create a key class with the proper attributes:
 - Key length: 256 bits.
 - Duration: For example, six months or whatever matches your policy.
 - Auto-key generation: Select to have keys automatically generated.

Note

Multiple Data Domain systems can share the same key class. For more information about key classes, see the section about RSA DPM key classes.

3. Create an identity using the Data Domain system's host certificate as its identity certificate. The identity and the key class have to be in the same identity group.
4. Import the certificates. See the section about importing certificates for more information.

About RSA DPM key classes

The Data Domain system retrieves a key from RSA DPM Key Manager by key class. A key class is a specialized type of security class used by the RSA DPM Key Manager that groups cryptographic keys with similar characteristics.

The RSA DPM Key Manager Server allows a key class to be set up to either return the current key, or to generate a new key each time. The Data Domain system supports only the key classes configured to return the current key. Do not use a key class that is configured to generate a new key each time.

Note

If the key length is not 256 bits, the DPM configuration will fail.

Importing the certificates

After obtaining certificates, import them to the Data Domain system.

Before you begin

- The Host certificate should be in PKCS12 format.
- The CA certificate should be in PEM format.
- You must obtain CA and Host certificates that are compatible with the RSA DPM Key Manager. You can request these certificates from third-party certificates authorities, or create them using appropriate SSL utility tools.
- If the system passphrase is not set, you cannot import the host certificate. The passphrase is set when you enable encryption. To change it, see the section regarding changing the system passphrase in the Managing the Data Domain Systems chapter.

DD OS supports certificates without any extension and certificates with server and client extensions for use with both the Data DD Manager and RSA DPM Key Manager. Certificates with client extensions are supported only by RSA DPM Key Manager, and certificates with server extensions are supported only by the DD System Manager.

DD OS does not support the RSA DPM Key Manager Server's Auto Registration Certificate capability, which uploads an auto registered certificate directly, or imports multiple certificates. This means that you must import the CA and Host certificates for a Data Domain system.

The following information describes how to respond to a couple of alerts that might appear during certificate management.

- If HTTPS fails to restart due to corrupted imported certificates, self-signed certificates are used. If this occurs, a managed alert, `UnusableHostCertificate`, is issued. To clear the alert, delete the corrupted certificates and re-import new certificates.
- If imported certificates are removed, for example during a system headswap and the imported certificates fail to copy over, a managed alert, `MissingHostCertificate`, is issued. Re-import the certificates to clear the alert.

After obtaining the certificates, import them to the Data Domain system as follows:

Procedure

1. Configure the RSA DPM Key Manager Server to use the CA and Host certificates. For instructions, see the *RSA DPM Key Manager Server Administration Guide*.
2. Import the certificates by redirecting the certificate files using `ssh` command syntax. See the *EMC Data Domain Operating System Command Reference Guide* for details.

```
ssh sysadmin@<Data-Domain-system> adminaccess certificate import {host
password password |ca } < path_to_the_certificate
```

For example, to import the host certificate `host.p12` from your personal computer's desktop over to the Data Domain system DD1 using `ssh`, enter:

```
# ssh sysadmin@DD1 adminaccess certificate import host password
abc123 < C:\host.p12
```

3. Import the CA certificate, for example, `ca.pem`, from your desktop to DD1 via SSH by entering:

```
# ssh sysadmin@DD1 adminaccess certificate import ca < C:\ca.pem
```

Performing this setup on the Data Domain system

Configure encryption on the Data Domain System Manager using the DPM Key Manager.

Procedure

1. Complete the DPM Key Manager setup on the RSA DPM Server.
2. The Data Domain system must be able to resolve its own IP address using its hostname. If this mapping has not been added to the DNS server, use this command line to add the entry to the `/etc/hosts` file:

```
# net hosts add ipaddr host-list
```

where *ipaddr* is the IP address of Data Domain system and *host-list* is the hostname of the Data Domain system.

If you are working in a dual stack environment, and the system displays the following error message: "RKM is not configured correctly," then use the `net hosts add ipaddr host-list` command to add the IPv4 address of the Data Domain System to the `/etc/hosts` file.

Note

A DPM server cannot be enabled in an environment using only IPv6 addresses.

Note

By default, the `fips-mode` is enabled. If the PKCS #12 client credential is not encrypted with the FIPS 140-2 approved algorithm, such as RC2, then you must disable `fips-mode`. See the *Data Domain Operating System Command Reference Guide* for information about disabling `fips-mode`.

3. Log into the DD System Manager and select the Data Domain system you are working with in the Navigation panel.

Note

Always perform DD System Manager functions on the system you have selected in the Navigation panel.

4. Click the **Data Management > File System > Encryption** tab.
5. Follow the instructions in the section regarding configuring encryption and select the **DPM Key Manager**. If encryption has already been set up, follow the instructions in the section regarding changing key managers after setup.

Changing key managers after setup

Select from the Embedded Key Manager or the RSA DPM Key Manager.

Before you begin

To manage certificates for a system, you must start DD System Manager on that system.

Procedure

1. Using the DD System Manager, select the Data Domain system you are working with in the Navigation panel.

2. Click **Data Management** > **File System** > **Encryption** tab.
3. Under Key Management, click **Configure**.
4. Enter your security officer username and password.
5. Select which Key Manager to use.
 - **Embedded Key Manager:** Select to enable or disable key rotation. If enabled, enter a rotation interval between 1-to-12 months. Select **Restart the file system now**, and click **OK**.
 - **RSA DPM Key Manager:** Enter the server name, key class, port (the default is 443), and whether the imported host certificate is FIPS compliant. The default mode is enabled. Select **Restart the file system now**, and click **OK**.
6. Click **Manage Certificates** to add certificates.

Managing certificates for RSA Key Manager

You must use both host and CA certificates with RSA Key Manager.

Note

Certificates are only necessary for RSA Key Manager. Embedded Key Manager does not use certificates.

Adding CA certificates for RSA Key Manager

Upload or copy and paste CA certificates.

Procedure

1. Select one of the following:
 - Select the option to upload a CA certificate as a .pem file and click **Browse** to find the file.
 - Select the option to copy and paste the CA certificate and paste the certificate contents into the field provided.
2. Click **Add** to add the certificate.

Adding a host certificate for RSA Key Manager

Upload the certificate as a .p12 file, or upload a public key as a .pem file and use a generated private key.

To start, select the first or second of the following steps:

Procedure

1. Select the option to upload the certificate as a .p12 file.
 - a. Enter a password.
 - b. Click **Browse** to find the .p12 file.
2. Select the option to upload the public key as a .pem file and use a generated private key.
 - a. Click **Browse** to find the .pem file.
3. Click **Add**.

Deleting certificates

Select a certificate with the correct fingerprint.

Procedure

1. Select a certificate to delete.
2. Click **Delete**.

The system displays a Delete Certificate dialog with the fingerprint of the certificate to be deleted.

3. Click **OK**.

Checking settings for encryption of data at rest

Check the settings for the Encryption feature.

Click the **Data Management** > **File System** > **Encryption** tabs. The currently used Key Manager is shown as Enabled. For a description of the Encryption settings, see the section about the encryption view.

Enabling and disabling encryption of data at rest

After configuring Encryption, the status is enabled and the Disabled button is active. When Encryption is disabled, the Enabled button is active.

Enabling encryption of data at rest

Use the DD System Manager to enable the Encryption feature.

Procedure

1. Using the DD System Manager, select the Data Domain system you are working with in the Navigation panel.
2. In the Encryption view, click the **Enable** button.
3. Both of the following options are available:
 - Select **Apply to existing data** and click **OK**. Encryption of existing data will occur during the first cleaning cycle after the file system is restarted.
 - Select **Restart the file system now** and click **OK**. Encryption will be enabled after the file system is restarted.

After you finish

Note

Applications may experience an interruption while the file system is restarted.

Disabling encryption of data at rest

Use the DD System Manager to disable the Encryption feature.

Procedure

1. Using the DD System Manager, select the Data Domain system you are working with in the Navigation panel.

2. In the Encryption view, click the **Disable** button.
The Disable Encryption dialog box is displayed.
3. In the Security Officer Credentials area, enter the user name and password of a security officer.
4. Select one of the following:
 - Select **Apply to existing data** and click **OK**. Decryption of existing data will occur during the first cleaning cycle after the file system is restarted.
 - Select **Restart the file system now** and click **OK**. Encryption will be disabled after the file system is restarted.

After you finish

Note

Applications may experience an interruption while the file system is restarted.

Locking and unlocking the file system

Use this procedure when an encryption-enabled Data Domain system (and its external storage devices) are being transported, or if you want to lock a disk that is being replaced. The procedure requires two accounts: Security Officer and System Administration roles.

Procedure

1. Using the DD System Manager, select the Data Domain system you are working with in the Navigation panel.
2. Go the File System Lock area of the **Data Management > File System > Encryption** view.
The Status shows whether the file system is Locked or Unlocked.
3. Disable the file system by clicking the **Disabled** button in the File System status area.
4. Use the procedure to lock or unlock the file system.

Locking the file system

To lock the file system, Encryption must be enabled and the file system must be disabled.

Procedure

1. Using the DD System Manager, select the Data Domain system you are working with in the Navigation panel.
2. Navigate to the File System Lock area of the **Data Management > File System > Encryption** view. Click **Lock File System**.
3. In the text fields of the Lock File System dialog box, provide:
 - The user name and password of a Security Officer account (an authorized user in the Security User group on that Data Domain system).
 - The current and a new passphrase.
4. Click **OK**.

This procedure re-encrypts the encryption keys with the new passphrase. This process destroys the cached copy of the current passphrase (both in-memory and on-disk).

Note

Changing the passphrase requires two-user authentication to protect against the possibility of a rogue employee's shredding the data.

⚠ CAUTION

Be sure to take care of the passphrase. If the passphrase is lost, you will never be able to unlock the file system and access the data. The data will be irrevocably lost.

5. Shut down the system:

⚠ CAUTION

Do not use the chassis power switch to power off the system. Enter the following command on the command line instead.

```
# system poweroff The 'system poweroff' command shuts down
the system and turns off the power. Continue? (yes|no|?)
[no]:
```

6. Transport the system or remove the disk being replaced.
7. Power on the system and use the procedure to unlock the file system.

Unlocking the file system

This procedure prepares an encrypted file system for use after it has arrived at its destination.

Procedure

1. Using the DD System Manager, select the Data Domain system you are working with in the Navigation panel.
2. Navigate to the **File System Lock** area of the **Data Management > File System > Encryption** view. Click **Unlock File System**.

The Unlock File System dialog box is displayed.

3. In the text fields, provide the passphrase that was used to lock the file system.
4. Click **OK**.

The Enable File System Status dialog box displays.

5. Click **Close** to exit.

If the passphrase is incorrect, the file system does not start and the system reports the error. Re-enter the correct passphrase, as directed in the previous step.

Changing the encryption algorithm

Reset the encryption algorithm if necessary, or select options to encrypt new and existing data or just new data.

Procedure

1. Using the DD System Manager, select the Data Domain system you are working with in the Navigation panel.

2. Go to the **Data Management > File System** and select the **Encryption** tab.
3. To change the Encryption Algorithm used to encrypt the Data Domain system, click **Change Algorithm**.

The Change Algorithm dialog box is displayed. Supported encryption algorithms are:

- AES-128 CBC
 - AES-256 CBC
 - AES-128 GCM
 - AES-256 GCM
4. Select an encryption algorithm from the drop-down list or accept the default AES 256-bit (CBC).

The AES 256-bit Galois/Counter Mode (GCM) is the most secure algorithm but it is significantly slower than the Cipher Block Chaining (CBC) mode.

Note

To reset the algorithm to the default AES 256-bit (CBC), click **Reset to default**.

5. Determine what data will be encrypted:
 - To encrypt existing and new data on the system, select **Apply to Existing data, Restart file system now**, and click **OK**. Existing data will be encrypted during the first cleaning cycle after the file system is restarted.

Note

Encryption of existing data can take longer than a standard file system clean operation.

- To encrypt only new data, select **Restart file system now** and click **OK**.
6. The status is displayed. Click **Close** when the process is complete.

Note

Applications may experience an interruption while the file system is restarted.
