

Dell DR Series System Command Line Reference Guide



Notes, Cautions, and Warnings



NOTE: A NOTE indicates important information that helps you make better use of your computer.



CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.



WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Copyright © 2014 Dell Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Dell™ and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

2014 - 04

Rev. A08

Contents

1 Introduction to the DR Series System Command Line Reference Guide.....	11
About the DR Series System CLI Documentation.....	11
Other Information You May Need.....	11
Contacting Dell.....	12
Locating Your System Service Tag.....	12
Documentation Feedback.....	12
2 Introducing the DR Series System.....	13
DR Series System Drive and System Capacities.....	14
Accessing the DR Series System CLI Commands.....	14
DR Series System CLI Commands Overview.....	14
3 Managing the DR Series System.....	17
Alerts Commands.....	17
Alerts Command Usage.....	17
alerts --show [--email].....	18
alerts --show [--snmp].....	18
alerts --show [--events] [--index <[-]number> [--count <number>] [--all].....	18
alerts --show [--alerts] [--index <[-] number>] [--count <number>] [--all].....	19
alerts --show [--summary].....	19
alerts --email [--add <email>].....	20
alerts --email [--daily_report <yes no>].....	20
alerts --email [--delete <email>].....	21
alerts --email [--recipients <email>].....	21
alerts --email [--relay_host <server name>].....	22
alerts --email [--admin_name <admin name>].....	22
alerts --email [--company <name>].....	22
alerts --email [--admin_email <email>].....	23
alerts --email [--phone <phone number>].....	23
alerts --email [--comments <text>].....	24
alerts --email [--appliance_alerts <yes no>].....	24
alerts --email [--software_updates <yes no>].....	24
alerts --email [--daily_report <yes no>].....	25
alerts --test_email.....	25
alerts --snmp_add --host <server name> --port <number> --community <name>.....	26
alerts --snmp_delete --host <server name>.....	26
alerts --snmp_disable --host <server name>.....	26
alerts --snmp_enable --host <server name>.....	26

alerts --snmp_trap_email [--enable] [--disable].....	27
alerts --help.....	27
Authenticate Commands.....	28
Authenticate Command Usage.....	28
authenticate --show [--users].....	28
authenticate --show [--domain <domain name>].....	29
authenticate --show [--login_group].....	29
authenticate --join --domain <domain name> [--ou <org-unit name>] --user <user name>.....	29
authenticate --leave [--user <user name>] [--force].....	30
authenticate --update --kerberos.....	30
authenticate --add [--user <user name>].....	31
authenticate --add [--login_group <DOMAIN\LOGIN GROUP>].....	31
authenticate --delete--user <user name>.....	31
authenticate --delete [--login_group <DOMAIN\LOGIN GROUP>].....	32
authenticate --set --user <user name>.....	32
authenticate --guestmode [--enable] [--disable].....	32
authenticate --guestmode [--enable].....	33
authenticate --guestmode [--disable].....	33
authenticate --server_signing --mode <auto mandatory disabled show>.....	33
authenticate --help.....	34
Network.....	35
Network Command Usage	35
network --show.....	36
network --delete.....	37
network --restart.....	37
network --setdhcp.....	38
network --setstatic_ip [--bondif <bondN>] [--nwif <ethN>] --ip <IPv4/IPv6 address> --netmask <netmask> [--gateway <IPv4/IPv6 address>].....	38
network --create_bond.....	38
network --create_eth.....	39
network --add_member.....	40
network --setdns [--suffix <dns suffix>] [--primary <IPv4/IPv6 address>] [--secondary <IPv4/IPv6 address>].....	40
network --setbonding --bondif <bondN> [--mode <ALB 802.3ad>] [--mtu <supported MTU range 512 - 9000>].....	40
network --update.....	41
network --factory_reset.....	42
network --host	42
network --route.....	42
network --nslookup --destination <ip address hostname>.....	43
network --traceroute --destination <ip address hostname>.....	43
network --ping --destination <ip address hostname> [--tries <number>] [--size <number>] [--interface <bondN ethN>].....	43
network --blink.....	45

network --enable	45
network --disable.....	45
network --troubleshoot [--links] [--gateway] [--ntp] [--dns] [--active_domain] [--nis] [--clients] [--port_mapper] [--network_config] [--show_active <nfs cifs ost rds>] [--interface <bondN ethN>].....	46
network --troubleshoot --gateway --interface <bondN ethN>.....	48
network --troubleshoot [--show_active <nfs cifs ost rds>].....	48
network --tcpdump [--port <nfs windows replication ost rds>] [--pkt_size <128 - 32768>] [--file_size <0 - 100>] [--stop] [--host <ip address list>] [--interface <bondN ethN>].....	48
network --tcpdump [--pkt_size <128 - 32768>].....	49
network --tcpdump [--file_size <0 - 100>].....	49
network --tcpdump [--host <ip address list>].....	49
network --tcpdump [--port <nfs windows replication ost rds>].....	50
network --iperf_client --server <ip address hostname> [--port <number>] [--window_size <num bytes [KB/ MB]>] [--interval <num seconds>] [--time <num seconds>].....	50
network --iperf_server [--port <number>] [--window_size <num bytes [KB/MB>].....	51
network --help.....	51
OST.....	54
OST Command Usage.....	54
ost --show [--config] [--file_history] [--name <name>] [--active_files] [--name <name>] [--clients] [--limits].....	54
ost --setpassword.....	56
ost --delete_client --name <OST Client Hostname>	56
ost --update_client --name <OST Client Hostname> --mode <auto passthrough dedupe>.....	57
ost --limit --speed <<num><kbps mbps gbps default> --target <ip address hostname>.....	57
ost --partial_images --containerid <Container id> [--delete <Partial image path>] [--timeout <0>].....	58
ost --help.....	58
RDA.....	59
RDA Command Usage.....	59
rda --show [--config] [--file_history] [--name <name>] [--active_files] [--name <name>] [--clients] [--limits].....	59
rda --setpassword.....	60
rda --delete_client --name <RDA Client Hostname>.....	61
rda --update_client --name <RDA Client Hostname> --mode <auto passthrough dedupe>.....	61
rda --limit --speed <<num><kbps mbps gbps> default> --target <ip address hostname>.....	61
rda --partial_images --containerid <Container id> [--delete <Partial image path>] [--timeout <0>].....	62
rda --help.....	62
Stats.....	63
Stats Command Usage	63
stats --system.....	64
stats --cpu.....	64
stats --memory.....	64
stats --network.....	65
stats --datacheck.....	66
stats --nfs.....	67

stats --cifs.....	68
stats --ost.....	69
stats --rds.....	70
stats --container --name <name>.....	71
stats --replication [--name <name>].....	71
stats --cleaner.....	72
stats --clients [--type <nfs cifs ost rds>].....	72
stats --reset [--nfs] [--cifs] [--ost] [--rds] [--datacheck].....	73
stats --reset --datacheck.....	73
stats --help.....	73
stats --datacheck.....	74
stats --datacheck Command Usage.....	75
stats --help datacheck.....	75
System.....	75
System Command Usage	75
system --show [--config]	76
system --show [--hardware].....	77
system --show [--storage] [--type <boot internal external>] [--service_tag <service tag>].....	77
system --show [--storage].....	79
system --show [--license] [--verbose].....	79
system --show [--ntp].....	79
system --show [--version].....	80
system --show [--timezones [Region]].....	80
system --show [--upgradefile]	81
system --show [--upgradehistory].....	81
system --show [--marker].....	81
system --show [--replication_traffic].....	81
system --show [--opdup_traffic].....	82
system --show [--backup_traffic].....	82
system --show [--mgmt_traffic].....	82
system --reboot.....	82
system --shutdown.....	83
system --upgrade.....	83
system --license [--validate] [--add].....	83
system --setname --name <node_name>.....	84
system --setcompression [--fast] [--best].....	85
system --setdate [--date <date>] [--timezone <Region/Zone>].....	85
system --setntp [--add <server name>].....	85
system --setntp [--delete <server name>].....	86
system --setntp [--enable].....	86
system --setntp [--disable].....	86
system --setntp [--adjust_time].....	87

system --setlogin.....	87
system --telnet [--enable --disable].....	87
system --datacheck [--enable <all namespace blockmap>].....	88
system --datacheck [--disable <all namespace blockmap>].....	88
system --datacheck [--throttle <1-100>].....	88
system --marker [--enable] [--disable].....	89
system --marker [--disable].....	89
system --marker [--enable].....	89
system --add_storage --enclosure <service tag>.....	90
system --storage [--blink] [--type <internal external>] [--service_tag <service tag>] [--disk <slot num>]	91
system --storage [--unblink] [--type <internal external>] [--service_tag <service tag>] [--disk <slot num>].....	91
system --mgmt_traffic	91
system --backup_traffic	92
system --replication_traffic.....	92
system --opdup_traffic	93
system --help.....	93
User.....	95
User Command Usage	95
user --show [--users] [--logins].....	96
user --enable --user <service root>.....	96
user --disable --user <service root>.....	96
user --help.....	97

4 Maintaining the DR Series System..... 99

Diagnostics.....	99
Diagnostics Command Usage	100
diagnostics --show.....	100
diagnostics --collect.....	100
diagnostics --collect [--name <name>].....	101
diagnostics --collect [--reason <reason>].....	101
diagnostics --collect [--force].....	101
diagnostics --collect [--dset].....	102
diagnostics --collect [--logs].....	102
diagnostics --collect [--cores].....	102
diagnostics --collect [--tcpdump].....	103
diagnostics --collect [--process_dump].....	103
diagnostics --collect [--all].....	103
diagnostics --delete [--name <name>].....	104
diagnostics --delete [--all].....	104
diagnostics --copy --name <name> --host <user@host ip>:<path>.....	104
diagnostics --help.....	105
Maintenance.....	105

Maintenance Command Usage.....	106
maintenance --filesystem [--scan_status].....	106
maintenance --filesystem [--scan_report [verbose]].....	107
maintenance --filesystem [--repair_status [verbose]]	107
maintenance --filesystem [--repair_history [verbose]].....	107
maintenance --filesystem [--scan_restart [verify_data verify_rda_metadata verify_metadata]].....	108
maintenance --filesystem [--repair_now].....	108
maintenance --filesystem [--reclaim_space].....	108
maintenance --filesystem [--stop_reclaim_space].....	109
maintenance --filesystem [--clear_quarantine].....	109
maintenance --filesystem [--start_scan [verify_data verify_rda_metadata verify_metadata]].....	109
maintenance --filesystem [--stop_scan].....	110
maintenance --configuration [--backup].....	110
maintenance --configuration [--restore]	110
maintenance --configuration [--reinit_dictionary].....	111
maintenance --hardware [--reinit_nvram].....	111
maintenance --hardware [--restore_hw_db].....	112
maintenance --hardware [--network_reconfigure].....	112
maintenance --hardware [--motherboard_replaced].....	112
maintenance --disk [--make_standby [slot num]] [--type <internal external-<num> service tag>] -- clear_foreign].....	113
maintenance --remote_access [--show].....	113
maintenance --remote access [--enable].....	114
maintenance --remote_access [--static_ip] [--ip <IPv4/IPv6 address>] [--netmask <netmask>] [--gateway <IPv4/IPv6 address>] [--device <lom1 lom2 lom3 lom4>].....	114
maintenance --remote access [--disable].....	114
maintenance --vdisk --check_consistency --type <boot internal external> [--service_tag <service tag>].....	114
maintenance --help.....	115

5 Managing DR Series System Storage Operations..... 117

System Storage Operation Commands.....	117
Connection.....	117
Connection Command Usage	117
connection --show [--name <name>]	118
connection --show [--name <name>] [--type <NFS CIFS OST RDS>] [--verbose].....	118
connection --show [--verbose].....	119
connection --add --name <name> --type <NFS CIFS OST RDS> [--clients <ip address>] [--rootmap <nobody root administrator>] [--options <nfs options>] [--capacity <positive integer>].....	120
connection --update --name <name> --type <NFS CIFS OST RDS> [--clients <ip address>] [--rootmap <nobody root administrator>] [--options <nfs options>] [--capacity <positive integer>].....	120
connection --delete --name <name> --type <NFS CIFS OST RDS> [--clients <ip address>].....	121
connection --enable --name <name> --type <NFS CIFS OST RDS>.....	121

connection --disable --name <name> --type <NFS CIFS OST RDS>.....	121
connection --help.....	122
Container.....	123
Container Command Usage	123
container --show.....	123
container --show [--name <name>] [--verbose].....	123
container --add --name <name>.....	124
container --delete --name <name>.....	124
container --delete --name <name> [--delete_files].....	125
container --marker [--enable <Auto CommVault Networker TSM ARCserve HP_DataProtector Unix_Dump BridgeHead>] [--disable <Auto CommVault Networker TSM ARCserve HP_DataProtector Unix_Dump BridgeHead>] --name <name>.....	125
container --delete_files --name <name>.....	126
container --help.....	126
Replication.....	127
Replication Command Usage	127
replication --show [--name <name>] [--role <source target>] [--verbose] [--limits].....	127
replication --show.....	128
replication --show [--limits].....	128
replication --add --name <name> --role <source target> --peer <ip address hostname> [--peer_name <name>] [--replication_traffic <ip address hostname>] [--encryption <none aes128 aes256>][--username <user name>].....	129
replication --update --name <name> --role <source target> [--peer <ip address hostname>] [--encryption <none aes128 aes256>] [--username <user name>].....	129
replication --delete --name <name> --role <source target> [--force].....	130
replication --start --name <name> --role <source target>.....	130
replication --stop --name <name> --role <source target>.....	131
replication --limit --speed <<num><kbps mbps gbps> default> --target <ip address hostname>.....	131
replication --resync --name <name> --role <source target>.....	131
replication --troubleshoot --peer <ip address hostname>.....	132
replication --help.....	132
Schedule.....	133
Schedule Command Usage.....	133
schedule --show [--cleaner].....	134
schedule --show [--replication] [--name <name>].....	134
schedule --add --day <day of the week> [--cleaner] [--replication] [--start_time <hh:mm>] [-- stop_time <hh:mm>] [--name <name>].....	134
schedule --delete --day <day of the week> [--cleaner] [--name <name>] [--replication].....	135
schedule --help.....	135
6 Data Integrity Checking.....	137
About Data Check.....	137

Priority Write Verify Scans.....	137
Continuous Data Verification Scans.....	138
Data Check CLI Commands.....	138
Data Check Options.....	138
Data Check CLI Commands.....	139
system --datacheck Commands.....	139
stats --datacheck Commands.....	139
System --Datacheck.....	139
System --Datacheck Command Usage.....	139
system --datacheck.....	140
system --datacheck [--disable <all namespace blockmap>].....	140
system --datacheck [--enable <all namespace blockmap>].....	140
system --datacheck [--throttle <1-100>].....	141
system --help datacheck.....	141
stats --datacheck.....	142
stats --datacheck Command Usage.....	142
stats --datacheck.....	142


7 Additional Linux Commands.....145

grep.....	145
Description.....	145
Syntax.....	145
Result.....	145
more.....	146
Description.....	146
Syntax.....	146
Results.....	146

Introduction to the DR Series System Command Line Reference Guide

About the DR Series System CLI Documentation

This topic introduces the concept of using the Dell DR Series system command line interface (CLI) method for managing your data backups, performing a variety of data storage operations, and using containers to meet your backup and replication storage needs.

 **NOTE:** The DR Series system CLI provides one method for managing the DR Series system, with the other being the DR Series system graphical user interface (GUI). In some instances, the DR Series system CLI may provide additional features and options that are not available in the DR Series system GUI and vice versa.


Other Information You May Need

 **WARNING:** For more information, see the safety and regulatory information that shipped with the DR Series system. Warranty information may be included within this document or as a separate document.


All documents listed are available at dell.com/support/manuals.

Document	Description
<i>Dell DR Series System Getting Started Guides</i>	Provide an overview of setting up the applicable DR Series system and technical specifications.
<i>Dell DR Series System Owner's Manuals</i>	Provide information about the applicable DR Series system features, troubleshooting the DR Series system, and installing or replacing the DR Series system components.
<i>Dell DR Series System Administrator Guide</i>	Provides information about managing backup and replication operations using the DR Series system GUI.
<i>Dell DR Series System Interoperability Guide</i>	Provides information on the supported hardware and software.

 **NOTE:** Always check for documentation updates at dell.com/support/manuals and read the updates first because they often supersede information in other documents.


 **NOTE:** Read the release notes first, because they contain the most recently documented information about known issues with a specific product release.

Contacting Dell

 **NOTE:** If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

1. Go to dell.com/contactdell.
2. Verify your country or region from the drop-down menu at the top left corner of the page.
3. Select your support category: **Technical Support**, **Customer Support**, **Sales**, or **International Support Services**.
4. Select the appropriate service or support link based on your requirement.

 **NOTE:** If you have purchased a Dell system, you may be asked for the Service Tag.

Locating Your System Service Tag


Your system is identified by a unique Express Service Code and Service Tag number. The Express Service Code and Service Tag are found on the front of the system by pulling out the information tag. This information is used by Dell to route support calls to the appropriate personnel.

Documentation Feedback

If you have feedback for this document, write to documentation_feedback@dell.com. Alternatively, you can click on the **Feedback** link in any of the Dell documentation pages, fill out the form, and click **Submit** to send your feedback.

Introducing the DR Series System

The DR Series system is a high-performance, disk-based backup and recovery appliance that is simple to deploy and manage.

 **NOTE:** Unless otherwise noted, later references to "the system" or "DR Series system" are used interchangeably to represent the Dell DR Series system.

The system has a simple installation process and is available in many drive capacities to fit SMB, enterprise, and remote office environments. For details, see [DR Series System Drive and System Capacities](#).

Using Dell deduplication and compression algorithm technology, the system can achieve data reduction levels ranging from 10:1 to 15:1. This reduction in data results in less incremental storage needs and a smaller backup footprint.

By removing redundant data, the system provides deduplication and compression that deliver:

- Fast, reliable backup and restore functionality.
- Reduced media usage and power and cooling requirements.
- Improved overall data protection and retention costs.

The benefits of data deduplication can be extended across the enterprise as well through the deduplicated replication function to provide a complete backup solution for multi-site environments.

Shorter Recovery Time Objectives (RTO) and more attainable Recovery Point Objectives (RPO) can also be assured as critical backup data remains on disk and online longer. Capital and administrative costs are diminished at the same time as internal service level agreements (SLAs) are more easily met.


The DR Series system includes the following:

- Advanced data protection and disaster recovery
- Simple management interface (using the system CLI)
- Adapts to a wide variety of data backup installations and environments

The Dell DR Series system contains data backup and management software preinstalled on a Dell hardware appliance, which provides a robust disk-based data deduplication backup capability installed on a deduplication-enabled appliance. The system supports two interface types, and the system software manages the storage containers using the following interfaces:

- Command line interface (CLI)
- Graphical user interface (GUI)

The DR Series system CLI provides the means for managing the status, data capacity, storage savings, and throughput of data containers.

 **NOTE:** An online data verification or data-checking feature called Data Check is enabled by default on the Dell DR Series system. For more information about Data Check, see [Data Integrity Checking](#).

This Dell DR Series system CLI documentation assumes that the DR Series system has been deployed in its network location, and it is ready to be accessed using the DR Series system CLI commands.

DR Series System Drive and System Capacities

The DR Series system comes in the following types:

- DR4000 system—which consists of preinstalled DR4000 system software on a modified Dell R510 appliance platform.
- DR4100 system—which consists of preinstalled DR4100 system software on a modified Dell R720xd appliance platform.
- DR6000 system—which consists of preinstalled DR6000 system software on a modified Dell R720xd appliance platform.

The internal system drive capacity and available physical capacities of the DR Series system vary, depending on your system type (DR4000, DR4100, etc.) and drives installed. For details, see:

- *Dell DR Series System Administrator Guide*—“Drive and Available Physical Capacities” and “DR Series Expansion Shelf”
- *Dell DR Series System Interoperability Guide*—“Expansion Unit Limits”

Accessing the DR Series System CLI Commands

To access the DR Series system CLI commands from the system CLI prompt, complete the following:

1. Launch a terminal emulation application and start the process for logging in to the DR Series system.
2. In **Host Name** (or **IP address**), type the host name or IP address for the DR Series system, and click **Open**.
3. At the system prompt, enter the username for the Administrator:
 - Type **administrator**
 - Press <Enter>
4. At the administrator password prompt, enter the password for the Administrator (the default is **St0r@ge!**):
 - Type **St0r@ge!**
 - Press <Enter>

The DR Series system administrator prompt is displayed.

5. At the administrator prompt, type **help**.
The DR Series system CLI commands are displayed. For more information, see the section DR Series System CLI Commands Overview.


DR Series System CLI Commands Overview

The following command groups are available. For more information on each command group, run `<command name> --help show`.

Table 1. DR Series System CLI Commands Overview

Command Group	Description
alerts	View system events and configure email notifications, contact information, and daily reports.
authenticate	Configure Active Directory (AD) authentication.
connection	Configure NFS CIFS OST RDS access to a container.

Command Group	Description
container	Configure a file system to share over NFS CIFS OST RDS.
diagnostics	Gather log information for support issues.
help	Display this help message.
maintenance	Repair the data and state of the system.
network	Configure networking properties.
ost	Configure OST for Symantec backup applications.
rda	Configure Rapid Data Access (RDA) for the Dell NetVault application.
replication	Manage replication between systems.
schedule	Manage replication and cleaner schedules in the system.
stats	View statistics for system components.
system	Manage and view the system configuration.
user	Enable or disable service and root accounts on the node.
grep	System tools
more	

 **NOTE:** The DR Series system Administrator account only provides access to the DR Series system CLI commands listed in this section. There is no access to Linux commands other than *grep* or *more* from the DR Series system command line with the Administrator account.

Managing the DR Series System

This topic introduces the DR Series system CLI commands for configuring, managing, and viewing the current status of a DR Series system. For example, the DR Series system CLI **alerts** and **system** commands both contain options that provide administrators with the capability to configure, manage, and display the status of the a DR Series system.

All of the CLI commands and command options that are displayed in the DR Series system are grouped together under the main command heading. The following list of commands provide the functionality for configuring, managing, and displaying the DR Series system status:

- **Alerts**
- **Authenticate**
- **Network**
- **OST** (OpenStorage Technology)
- **RDA** (Rapid Data Access)
- **Stats** (statistics)
- **System**
- **User**

Alerts Commands

This topic introduces the set of DR Series system CLI commands that enable you to perform the following tasks:


- Display system alerts and events.
- Create new email accounts or modify existing email accounts for recipients, which are used for email alert notifications.
- Select to receive notifications about appliance alerts and software updates.
- Test to confirm that email account recipients can receive alerts via Simple Network Management Protocol (SNMP) traps for a designated host.
- Set, enable, disable, or delete SNMP traps for a designated host.

Alerts Command Usage

This topic introduces the **alerts** command usage:

- **alerts --show [options]**
- **alerts --email [options]**
- **alerts --test_email**
- **alerts --snmp_add [options]**
- **alerts --snmp_delete --host <server name>**
- **alerts --snmp_enable --host <server name>**
- **alerts --snmp_disable --host <server name>**
- **alerts --snmp_trap_email [options]**

- **alerts --help**

 **NOTE:** If you specify a command without supplying the expected value or option, you will be prompted to provide the correct value or option.

alerts --show [--email]

Description

Displays the list of email recipients, mail relay host, and the administrator contact information for the DR Series system.

Syntax

```
alerts --show --email
```

Result

```
Recipients:      john_smith@acme.com
Relay Host:      10.10.10.10
Admin Name:      John Smith
Company Name:    Acme.com
Admin Email:     john_smith@acme.com
Phone:           408-555-1212
Comments:        Day Shift Administrator
```

alerts --show [--snmp]

Description


Displays the current SNMP information for a DR Series system.

Syntax

```
alerts --show --snmp
```

Result


Host	Status	Port	Community
10.20.20.10	Enabled	2100	snmpPublic
10.25.19.11	Enabled	1120	snmpPublic12
10.12.14.20	Enabled	1550	snmpPublic11

 **NOTE:** For more information about configuring a host to receive SNMP alerts, see [alerts --email \[--relay_host <server name>\]](#).

alerts --show [--events] [--index <[-]number> [--count <number>] [--all]

Description

Displays the current list of system events.

 **NOTE:** The default is to display the 32 most recent events (this example is intentionally brief). The count and index options can also be used to filter the list of events (**alerts --show --events --index <number>** or **alerts --show --events --index <number>**).

Syntax

```
alerts --show --events
```

Result


Index	Severity	Event Message
Time		

-			
399	INFO	2012-06-10 14:07:18	System
diagnostic package collected.			
398	INFO	2012-06-10 12:21:47	Successfully
updated Cleaner schedule.			
397	INFO	2012-06-10 12:20:03	User service
enabled.			

alerts --show [--alerts] [--index <[-] number>] [--count <number>] [--all]

Description

Displays the current list of DR Series system alerts.

 **NOTE:** By default, all DR Series system alerts are displayed.

Syntax

```
alerts --show --alerts
```

Result

Index
1

Time
2012-06-19 18:19:09

Alert Message
Network Interface Controller Embedded (LOM) Port 1 disconnected. Reconnect it to a network and/or check your network switches or routers for network connectivity issues.

Index
2

Time
2012-06-19 18:19:09

Alert Message
Network Interface Controller PCI Slot 1 Port 0 disconnected. Reconnect it to a network and/or check your network switches or routers for network connectivity issues.

Index
3

Time
2012-06-19 18:19:09

Alert Message
Network Interface Controller PCI Slot 1 Port 1 disconnected. Reconnect it to a network and/or check your network switches or routers for network connectivity issues.

alerts --show [--summary]

Description

Displays a summary list of DR Series system alerts.

Syntax

```
alerts --show --summary
```

Result

```
Total alert messages:      5
Total event messages:     42
Last event index:         42
```

alerts --email [--add <email>]

Description

Displays the current email recipient address(es) for the DR Series system.

Syntax

```
alerts --email
```

Result

```
Recipients:      john_smith@acme.com
Relay Host:      10.10.10.10
Admin Name:      John Smith
Company Name:    Acme.com
Admin Email:     john_smith@acme.com
Phone:          408-555-1212
Comments:       Day Shift Administrator
```

Description

To configure and add a new email recipient address (for example, Juan Ruiz). The recipient is included in the cc: field of email notifications.

If the email address contains special characters (such as #), enclose the email address in double quotation marks. For example, `alerts --email --add "#IT_team@acme.com"`.

Syntax

```
alerts --email --add juan_ruiz@acme.com
```

Results

```
Alert email settings updated.
Recipients:      john_smith@acme.com;juan_ruiz@acme.com
Relay Host:
Admin Name:      John Smith
Company Name:    Acme.com
Admin Email:     john_smith@acme.com
Phone:          408-999-555-1212
Comments:       Day Shift Administrator
```

alerts --email [--daily_report <yes | no>]

Description

Configures the “yes/no” setting for sending daily statistics about each container to the administrator of a DR Series system. Setting this option to **yes** causes the system administrator to receive email notifications containing the statistics for the last 24 hours for each container (setting this option to **no** means that the system administrator will not receive daily email notifications about container statistics).

Syntax

```
alerts --email --daily_report <yes|no>

    --yes  Enables daily container stats notification on DR.
    --no   Disables daily container stats notification on DR.
```

Result

```
alerts --email --daily_report yes

Alert email settings updated.
Daily container stats notification has been enabled.
Recipients           : juan_corona@acme.com
Relay Host           : acme-sys-60.western.local
Admin Name           : Juan Corona
Company Name         : Acme Inc.
Admin Email          : juan_corona@acme.com
Phone                : 438-999-6699
Comments             : Days shift1 administrator
Appliance Alerts     : Yes
Software Updates     : Yes
Email SNMP Trap's    : No
Email Daily container stats : Yes
```

alerts --email [--delete <email>]

Description

Deletes an existing email recipient address (for example, Juan Ruiz) for the DR Series system. If the email address contains special characters (such as #), enclose the email address in double quotation marks. For example, `alerts --email --delete "#IT_team@acme.com"`.

Syntax

```
alerts --email --delete juan_ruiz@acme.com
```

Result

```
Alert email settings updated.
Recipients:   john_smith@acme.com
Relay Host:
Admin Name:   John_Smith
Company Name: Acme.com
Admin Email:  john_smith@acme.com
Phone:       408-555-1212
Comments:    Day Shift Administrator
```

alerts --email [--recipients <email>]

Description

Configures the email addresses for all recipients designated to receive alert email notifications for the DR Series system. Recipients are included in the cc: field of email notifications. If you want to include more than one email address, separate them with a comma.

If an email address contains special characters (such as #), enclose the email address in double quotation marks. For example, `alerts --email --recipients "#IT_team@acme.com", juan_ruiz@acme.com"`.

Syntax

```
alerts --email --recipients john_smith@acme.com, juan_ruiz@acme.com
```

Result

```
Alert email settings updated.
Recipients:      john_smith@acme.com;juan_ruiz@acme.com
Relay Host:
Admin Name:      John_Smith
Company Name:    Acme.com
Admin Email:     john_smith@acme.com
Phone:          408-555-1212
Comments:       Day Shift Administrator
```

alerts --email [--relay_host <server name>]

Description

Configures the mail relay host used in sending the alert email notifications for the DR Series system.

Syntax

```
alerts --email --relay_host relayhost13
```

Result

```
Alert email settings updated.
Recipients:      john_smith@acme.com;juan_ruiz@acme.com
Relay Host:      relayhost13
Admin Name:      John_Smith
Company Name:    Acme.com
Admin Email:     john_smith@acme.com
Phone:          408-555-1212
Comments:       Day Shift Administrator
```

alerts --email [--admin_name <admin name>]

Description

Configures an administrator name (**admin_name**) for the DR Series system.

Syntax

```
alerts --email --admin_name John_Smith
```

Result

```
Alert email settings updated.
Recipients:
Relay Host:      relayhost13
Admin Name:      John_Smith
Company Name:
Admin Email:
Phone:
Comments:
```



NOTE: To enable the use of spaces between the first and last name values when configuring an administrator name (or between multiple words in **--company <name>**, and in **--comments <text>**), enclose these values within quotation marks (for example, using the command string, **--admin_name "John Smith"**).

alerts --email [--company <name>]

Description

Configures a company name to associate with the DR Series system.

Syntax

```
alerts --email --company Acme.com
```

Result

```
Alert email settings updated.
Recipients:
Relay Host:      relayhost13
Admin Name:     John_Smith
Company Name:   Acme.com
Admin Email:
Phone:
Comments:
```

alerts --email [--admin_email <email>]

Description

Configures the email account for the administrator associated with the DR Series system. The administrator is displayed in the From: field and included in the To: field of email notifications. If you want to include more than one email address, separate them with a comma. For example, `alerts --email --admin_email john_smith@acme.com,juan_ruiz@acme.com`.

If the email address contains special characters (such as #), enclose the email address in double quotation marks. For example, `alerts --email --admin_email "#IT_admin@acme.com"`.

Syntax

```
alerts --email --admin_email john_smith@acme.com
```

Result

```
Alert email settings updated.
Recipients:
Relay Host:      relayhost13
Admin Name:     John_Smith
Company Name:   Acme.com
Admin Email:    john_smith@acme.com
Phone:
Comment:
```

alerts --email [--phone <phone number>]

Description

Configures the telephone number for the administrator associated with the DR Series system.

Syntax

```
alerts --email --phone 408-999-5555
```

Result

```
Alert email settings updated.
Recipients:
Relay Host:      relayhost13
Admin Name:     John_Smith
Company Name:   Acme.com
Admin Email:    john_smith@acme.com
Phone:         408-999-5555
Comments:
```

alerts --email [--comments <text>]

Description

Adds comments that help define or describe the administrator associated with the DR Series system.

Syntax

```
alerts --email --comments Day Shift Administrator
```

Result

```
Alert email settings updated.
Recipients:
Relay Host:      relayhost13
Admin Name:     John_Smith
Company Name:   Acme.com
Admin Email:    john_smith@acme.com
Phone:         408-999-5555
Comments:      Day Shift Administrator
```

alerts --email [--appliance_alerts <yes | no>]

Description

Configures the “yes/no” setting for sending email notifications to the administrator of a DR Series system when there are alerts for the system appliance. Setting this option to **yes** causes the system administrator to receive email notifications when there are system appliance alerts (setting this option to **no** means that the system administrator will not receive email notifications about system appliance alerts).

Syntax

```
alerts --email --appliance_alerts yes
```

Result

```
Alert email settings updated.
Recipients           : juan_corona@acme.com
Relay Host           : acme-sys-60.western.local
Admin Name           : Juan Corona
Company Name         : Acme Inc.
Admin Email          : juan_corona@acme.com
Phone                : 438-999-6699
Comments             : Days shift1 administrator
Appliance Alerts     : Yes
Software Updates     : Yes
Email SNMP Trap's    : No
Email Daily container stats : Yes
```

alerts --email [--software_updates <yes | no>]

Description

Configures the “yes/no” setting for sending email notifications to the administrator of a DR Series system when there are updates for the system software installed on the system appliance. Setting this option to **yes** causes the system administrator to receive email notifications when there are system software updates (setting this option to **no** means that the system administrator will not receive email notifications about system software updates).

Syntax

```
alerts --email --software_updates yes
```

Result

```
Alert email settings updated.
Recipients                : juan_corona@acme.com
Relay Host                 : acme-sys-60.western.local
Admin Name                 : Juan Corona
Company Name               : Acme Inc.
Admin Email                : juan_corona@acme.com
Phone                      : 438-999-6699
Comments                   : Days shift1 administrator
Appliance Alerts          : Yes
Software Updates           : Yes
Email SNMP Trap's         : No
Email Daily container stats : Yes
```

alerts --email [--daily_report <yes | no>]

Description

Configures the “yes/no” setting for sending daily statistics about each container to the administrator of a DR Series system. Setting this option to **yes** causes the system administrator to receive email notifications containing the statistics for the last 24 hours for each container (setting this option to **no** means that the system administrator will not receive daily email notifications about container statistics).

Syntax

```
alerts --email --daily_report <yes|no>

    --yes  Enables daily container stats notification on DR.
    --no   Disables daily container stats notification on DR.
```

Result


```
alerts --email --daily_report yes

Alert email settings updated.
Daily container stats notification has been enabled.
Recipients                : juan_corona@acme.com
Relay Host                 : acme-sys-60.western.local
Admin Name                 : Juan Corona
Company Name               : Acme Inc.
Admin Email                : juan_corona@acme.com
Phone                      : 438-999-6699
Comments                   : Days shift1 administrator
Appliance Alerts          : Yes
Software Updates           : Yes
Email SNMP Trap's         : No
Email Daily container stats : Yes
```

alerts --test_email

Description

Sends a test email alert notification to all of the configured email recipients in the DR Series system.

 **NOTE:** Verify that the configured email recipients received the test email notifications that were sent. This is an important check that proves that the designated email recipients can receive DR Series system alert notifications.

Syntax

```
alerts --test_email
```

Result

Test email sent.

alerts --snmp_add --host <server name> --port <number> --community <name>**Description**

Sets SNMP traps for a host by defining its host name, port number, and listing the corresponding SNMP community.

Syntax

```
alerts --snmp_add --host 10.12.14.20 --port 1550 --community snmpPublic1
```

Result

Host "10.12.14.20" added to SNMP alert recipients.

alerts --snmp_delete --host <server name>**Description**

Deletes SNMP traps for a host by identifying it by name or IP address at the DR Series system prompt.

Syntax

```
alerts --snmp_delete --host 10.10.10.12
```

Result

Host "10.10.10.12" deleted from SNMP alert recipients.

alerts --snmp_disable --host <server name>**Description**

Disables SNMP traps for a host by identifying it by name or IP address at the DR Series system prompt.

Syntax

```
alerts --snmp_disable --host 10.12.14.20
```

Result

Host "10.12.14.20" disabled for SNMP alerts.

alerts --snmp_enable --host <server name>**Description**

Enables SNMP traps for a host by identifying it by name or IP address at the DR Series system prompt.

Syntax

```
alerts --snmp_enable --host 10.12.14.20
```

Result

Host "10.12.14.20" enabled for SNMP alerts.

alerts --snmp_trap_email [--enable] [--disable]

Description


Enables or disables SNMP traps to be sent out as an email message.

Syntax

```
alerts --snmp_trap_email --enable
```

Result

Successfully enabled SNMP Trap email forwarding.

 **NOTE:** To disable SNMP trap mail forwarding, substitute the **--disable** command, as in the following example:

```
alerts --snmp_trap_email --disable
Successfully disabled SNMP Trap email forwarding.
```

alerts --help

Description

Displays the listing of alerts and related options that can be used as a reference when using the DR Series system CLI.

Syntax

```
alerts --help
```

Result

Usage:

```
alerts --show [--email]
    [--snmp]
    [--events] [--index <[-]number>] [--count <number>] [--all]
    [--alerts] [--index <[-]number>] [--count <number>] [--all]
    [--summary]

alerts --email [--add <email>]
    [--delete <email>]
    [--recipients <email>]
    [--relay_host <server name>]
    [--admin_name <admin name>]
    [--company <name>]
    [--admin_email <email>]
    [--phone <phone number>]
    [--comments <text>]
    [--appliance_alerts <yes|no>]
    [--software_updates <yes|no>]
    [--daily_report <yes|no>]

alerts --test_email
alerts --snmp_add --host <server name>
    --port <number>
    --community <name>

alerts --snmp_delete --host <server name>

alerts --snmp_enable --host <server name>

alerts --snmp_disable --host <server name>

alerts --snmp_trap_email [--enable][--disable]
```

```

alerts --help

alerts <command> <command-arguments>
<command> can be one of:
--show           Displays system alerts and events.
--test_email     Sends a test email using current email settings.
--snmp_add       Sets SNMP traps to be sent to a host.
--snmp_delete    Stops sending SNMP traps to a host.
--snmp_enable    Enables SNMP traps for a host.
--snmp_disable   Disables SNMP traps for a host.
--snmp_trap_email Enables/Disables SNMP traps to be sent out as an email.

```

For command-specific help, please type `alerts --help <command>`
For example:
`alerts --help show`

Authenticate Commands


This topic introduces the set of DR Series system CLI commands that let you configure the DR Series system so it can authenticate with the Microsoft Windows Active Directory Services (ADS).

For information about specific **authenticate** commands, see [Authenticate Command Usage](#).

Authenticate Command Usage

This topic introduces the **authenticate** command usage:


- **authenticate --show [options]**
- **authenticate --join [options]**
- **authenticate --leave [options]**
- **authenticate --update --kerberos**
- **authenticate --add [options]**
- **authenticate --delete [options]**
- **authenticate --set --user <user name>**
- **authenticate --guestmode [options]**
- **authenticate --server_signing --mode <auto|mandatory|disabled|show>**
- **authenticate --help**

 **NOTE:** If you specify a command without supplying the expected value or option, you will be prompted to provide the correct value or option.

authenticate --show [--users]

Description

Displays the current status of the Microsoft Active Directory Service (ADS) domain, or if it is not joined, it can display the status of any authorized local CIFS user. For more information, see the [authenticate --show \[--domain <domain name>\]](#).

 **NOTE:** If this command is entered, but the DR Series system has not joined the ADS to any domain, the following message is displayed.

```
This system has not joined any domain.
```

Syntax

```
authenticate --show
```

Result

```
Domain: ads.storage.local
```


If you have joined the ADS to a designated domain and you want to see the authorized users, enter the **authenticate --show --users** command to display the current status:

```
authenticate --show --users
administrator2
administrator
```

authenticate --show [--domain <domain name>]

Description

Displays the current status of the Active Directory Services (ADS) domain to which the DR Series system is joined.

 **NOTE:** If you have not joined the DR Series system to an ADS domain, use the DR Series system CLI **authenticate --join --domain** command. For more information, see [authenticate --join --domain <domain name> \[--ou <org-unit name>\] --user <user name>](#).

Syntax

```
authenticate --show --domain acme-ad.acme.local
```

Result

```
Domain Name                : acme-ad.acme.local
Domain Controller Time     : 2012-10-19 12:13:40 PDT
System Time                : 2012-10-19 12:13:40 PDT
Time Skew                  : 0 secs
Domain Controller Name     : test-ad-2008r2.acme-ad.acme.local
Domain Controller Address  : 10.20.20.4
```

authenticate --show [--login_group]

Description

Displays the currently enabled and authenticated login group on a Microsoft Active Directory Services domain.

Syntax

```
authenticate --show --login_group
```


Result


```
Login group: acmeADS\Domain Admins
```

authenticate --join --domain <domain name> [--ou <org-unit name>] --user <user name>

Description

Joins the DR Series system to an Active Directory Services (ADS) domain when you specify the ADS domain name and a valid user (administrator) for that domain.

 **NOTE:** When attempting to join the ADS domain, the administrator password is required for that domain to ensure that the join operation is successful. Supported domain names are limited to 64 characters in length and can only consist of a combination of A-Z, a-z, 0-9, and two special characters: a dash (-) and a period (.).


 **NOTE:** If you had previously joined the DR Series system to an ADS domain before running Restore Manager (RM), after it completes you must manually rejoin the desired ADS domain using the **authenticate --join** command.

Syntax

```
authenticate --join --domain ads.storage.local --user administrator
```

Result

```
Enter password for administrator@ads.storage.local:
Successfully joined domain ads.storage.local
Disabling NTP service... done.
Updated Windows Access Server Configuration.
Updated Kerberos configuration.
Updated machine password.
Updated DNS.
Restarting Windows Access Server... done.
```

 **NOTE:** The **--ou** command is optional and allows for defining a specific organizational group in the ADS that may require its own administrative access rights (such as an executive management or finance group).

authenticate --leave [--user <user name>] [--force]

Description


Enables a DR Series system to leave a Microsoft Active Directory Services (ADS) domain when you provide a valid administrator password.

Syntax

```
authenticate --leave --user administrator
```

Result

```
Enter password for administrator@ads.storage.local:
Successfully left domain ads.storage.local.
Updated Windows Access Server configuration.
Updated Kerberos configuration
Restarting Windows Access Server... done.
Enabling NTP service... done.
```

 **NOTE:** The **--force** command is optional and allows the DR Series system to leave the ADS domain when communication between the system and the ADS domain is lost and the **--leave** operation is pending or in progress.

authenticate --update --kerberos

Description

Updates a Microsoft Active Directory Service (ADS) Kerberos configuration (Kerberos is a computer network authentication protocol).

Syntax

```
authenticate --update --kerberos
```

Result

Updated kerberos configuration.

authenticate --add [--user <user name>]

Description

Adds a new local CIFS workgroup user for CIFS authentication (and administrative tasks) after you provide and confirm the CIFS user password.

Syntax

```
authenticate --add --user administrator2
```

Result

```
Enter password for new CIFS user administrator2:
Re-enter password for new CIFS user administrator2:
Added CIFS user administrator2.
```

authenticate --add [--login_group <DOMAIN\LOGIN GROUP>]

Description

Adds an authenticated login group in an Active Directory Services (ADS) domain in accordance with the following ADS login group guidelines:

- Log in as an administrator via the CLI, and use SSH, Telnet, or a local console connection as a domain\user that is part of a login group. When you log in as an administrator via the CLI, you are prompted to use the credentials of the user account by which you log in (for example: if you log in as a Domain\administrator, you need to respond using these credentials).
- Log in as an administrator via the GUI, and use a web interface connection as a domain\user that is part of a login group (when this has been enabled via the CLI).
- If no login group is specified, or the group is disabled, no access using domain accounts is permitted.
- Adding a login group can only be enabled via the CLI.
- Adding a login group is only possible when the DR Series system is already joined to a domain.
- If the login group name has a space in it, it must be contained within double-quotation marks (" ").
- When adding a login group, it must use the naming convention of Domain\group name.
- The login group must exist in the domain before you can add it (a check is performed to verify that the group exists in ADS).
- Changes made to the login group take effect on the next log in attempt (no active checking is done on group, which matches how Windows ADS works).

 **NOTE:** To delete an existing login group, see [authenticate --delete \[--login_group <DOMAIN\LOGIN GROUP>\]](#).

Syntax

```
authenticate --add --login_group "acmeads\Domain Admins"
```

Result

Successfully added login group acmeads\Domain Admins.

authenticate --delete--user <user name>

Description

Deletes an existing local CIFS workgroup user from CIFS authentication (and administrative tasks).

Syntax

```
authenticate --delete --user administrator2
```


Result

Deleted CIFS user administrator2.

authenticate --delete [--login_group <DOMAIN\LOGIN GROUP>]

Description

Deletes an existing authenticated login group in an Active Directory Services (ADS) domain. For more information about DR Series system and ADS login group guidelines, see [authenticate --add \[--login_group <DOMAIN\LOGIN GROUP>\]](#).

 **NOTE:** Ensure that the login group exists in the Active Directory Services (ADS) domain, and that the “\” and any spaces in the login group name are in quotation marks (“ ”).

Syntax

```
authenticate --delete --login_group "acmeads\Domain Admins"
```

Result

Deleted login group acmeads\Domain Admins.

authenticate --set --user <user name>

Description


Sets the password for an existing local CIFS workgroup user when you create and confirm the new password.

Syntax

```
authenticate --set --user administrator2
```

Result

```
Enter new password for CIFS user administrator2:
Re-enter new password for CIFS user administrator2:
Changed administrator2's password.
```

 **NOTE:** The DR Series system administrator that manages the DR Series system has a different set of privileges than does the CIFS user administrator. For example, only the DR Series system administrator can change the password for the CIFS user administrator.

authenticate --guestmode [--enable] [--disable]

Description

Configures all CIFS shares for guest-only access by enabling or disabling this capability. For specific examples of enabling or disabling guest-only access, see [authenticate --guestmode --enable](#) and [authenticate --guestmode --disable](#).

Syntax

```
authenticate --guestmode
```

Result

Must include either enable or disable option.
--guestmode - Configures all CIFS shares for guest only access.

Usage:

```
authenticate --guestmode [--enable]
                [--disable]
```

```
--enable      Enable only guest access CIFS shares.
--disable     Disable only guest access for CIFS shares.
```

authenticate --guestmode [--enable]

Description


Configures all CIFS shares for guest-only access.

Syntax

```
authenticate --guestmode --enable
```

Result

```
Restarting Windows Access Server... done.
```

 **NOTE:** If you attempt to enable guestmode for all CIFS shares when the DR Series system is already joined to an ADS domain by (using the DR Series system CLI **authenticate --guestmode --enable** command), the following error message displays: *This node is already joined to domain <domainname>. Please leave the domain before enabling the guest-only mode.*

authenticate --guestmode [--disable]

Description

Disables all CIFS shares as guest-only access.

Syntax

```
authenticate --guestmode --disable
```

Result

```
Restarting Windows Access Server... done.
```

 **NOTE:** If you attempt to enable guestmode for all CIFS shares when the DR Series system is already joined to an ADS domain (using the DR Series system CLI **authenticate --guestmode --enable** command), the following error message displays: *This node is already joined to domain <domainname>. Please leave the domain before enabling the guest-only mode.*

authenticate --server_signing --mode <auto | mandatory | disabled | show>

Description

Configures the server signing for Common Internet File System (CIFS) on a DR Series system. This is a security provision based on Server Message Block (SMB) signing, a form of packet authentication. After CIFS-based users are authenticated, SMB signing adds a digital signature to each packet that is transferred between client and server. These digital signatures verify that the identity of the server matches the credentials expected by the client, and vice versa. By verifying that every packet that is received comes from an authenticated source, these digital signatures ensure the integrity of the communications. The DR Series system CLI **--server_signing --mode** command contains four values:

- **auto** — Configures authentication via server signing to be automatically performed.
- **mandatory** — Configures authentication via server signing as mandatory, or the connection will be dropped.

- **disabled** — Disables authentication via server signing so that no connections are accepted.
- **show** — Displays the current server signing settings.

Syntax

```
authenticate --server_signing --mode auto
```

Result

Successfully added server signing to auto.

authenticate --help

Description

Displays the list of all authenticate-related options that can be used as a reference when using the DR Series system CLI.

Syntax

```
authenticate --help
```

Result

Usage:

```
authenticate --show [--users]
                [--domain <domain name>]
                [--login_group]
```

```
authenticate --join --domain <domain name>
                [--ou <org-unit name>]
                --user <user name>
```

```
authenticate --leave [--user <user name>]
                [--force]
```

```
authenticate --update --kerberos
```

```
authenticate --add [--user <user name>]
                [--login_group <DOMAIN\LOGIN GROUP>]
```

```
authenticate --delete [--user <user name>]
                [--login_group <DOMAIN\LOGIN GROUP>]
```

```
authenticate --set --user <user name>
```

```
authenticate --guestmode [--enable]
                [--disable]
```

```
authenticate --server_signing --mode <auto|mandatory|disabled|show>
```

```
authenticate --help
```

```
authenticate <command> <command-arguments>
```

<command> can be one of:

```
--show          Displays current ADS domain, authorized local CIFS users, and
login group.
--join          Joins an ADS domain.
--leave         Leaves an ADS domain.
--update        Updates ADS configuration.
--add           Creates local workgroup user for CIFS authentication or adds
login group.
--delete        Deletes local workgroup user from CIFS authentication or
deletes login group.
```

```
--set          Sets password for a local workgroup user.
--guestmode    Configures all CIFS shares for guest only access.
--server_signing Configures server signing for CIFS.
```

For command-specific help, please type `authenticate --help <command>`

For example:
`authenticate --help show`

Network


The DR Series system CLI commands let you perform the following network-related tasks:


- Displays information about a DR Series system.
- Deletes network interfaces.
- Restarts networking.
- Configures bond interface to use DHCP.
- Assigns a static IP address to the bond interface.
- Creates bond interfaces for the system.
- Creates eth interfaces for the system.
- Adds an interface to an existing bond.
- Configures servers in the domain name system (DNS).
- Updates the bonding mode or maximum transmission unit (MTU).
- Updates bonding and individual interface information.
- Resets networking to factory configuration.
- Manages local hosts.
- Manages local routes.
- Looks up the IP address or hostname for a specific destination.
- Starts a packet trace route for a specific network host.
- Pings a destination host
- Blinks LED on the specific ethernet device.
- Starts the specific ethernet devices on restart.
- Does not start the specific ethernet devices on restart.
- Performs basic troubleshooting.
- Capture network traffic.
- Runs iperf (Network Performance) in client mode.
- Runs iperf (Network Performance) in server mode.

Network Command Usage

- **network --show [options]**
- **network --delete**
- **network --restart**
- **network --setdhcp [options]**
- **network --setstatic_ip [options]**
- **network --create_bond**
- **network --create_eth**
- **network --add_member**

- `network --setdns [options]`
- `network --setbonding [options]`
- `network --update`
- `network --factory_reset`
- `network --host`
- `network --route`
- `network --nslookup [options]`
- `network --traceroute [options]`
- `network --ping [options]`
- `network --blink`
- `network --enable`
- `network --disable`
- `network --troubleshoot [options]`
- `network --tcpdump [options]`
- `network --iperf_client [options]`
- `network --iperf_server [options]`
- `network --help`

 **NOTE:** If you specify a command without supplying the expected value or option, you are prompted to provide the correct value or option.

 **NOTE:** Most network commands require a `network --restart` command for the changes to occur.

network --show

Description

Displays the current networking configuration for a DR Series system.

Syntax

```
network --show [--bondif <bond0,bond1,...,bondN>] [--nwif <eth0,eth1,...,ethN>]
[--hosts] [--routes] [--interface <bondN|ethN>]
```

```
--bondif      Bond interface(s) to show.
--nwif        Eth interface(s) to show.
--hosts       Show local host.
--routes      Show local routes.
--interface   Routes for a specific interface.
```

Result

```
Device                : bond0
Enabled                : yes
Link                   : yes
Boot protocol         : dhcp
IP Addr                : 10.20.24.55
Netmask                : 255.255.252.0
Gateway                : 10.20.32.13
MAC Addr               : 78:2B:CB:47:D0:08
MTU                    : 1500
Bonding options       : "mode=balance-alb miimon=100 xmit_hash_policy=2"
Slave Interfaces      : eth0,eth1,eth2,eth3
eth0 MAC               : 78:2B:CB:47:D0:08
eth0 Max Speed        : 1000baseT/Full
eth0 Speed             : 1000Mb/s
eth0 Duplex            : Full
```

```

eth1 MAC                : 00:50:56:93:5A:02
eth1 Max Speed          : 1000baseT/Full
eth1 Speed              : 1000Mb/s
eth1 Duplex             : Full
eth2 MAC                : 00:50:56:93:5A:03
eth2 Max Speed          : 1000baseT/Full
eth2 Speed              : 1000Mb/s
eth2 Duplex             : Full
eth3 MAC                : 00:50:56:93:5A:04
eth3 Max Speed          : 1000baseT/Full
eth3 Speed              : 1000Mb/s
eth3 Duplex             : Full
DNS Suffix              : storage.local
Primary Nameserver      : 10.25.19.15
Secondary Nameserver    : 10.25.19.16

```

network --delete

Description

The command deletes a network interface.

Syntax

```

network --delete      [--bondif <bond0,bond1,...,bondN>]
                    [--member <eth0,eth1,...,ethN>]
                    [--nwif <eth0,eth1,...,ethN>]

                    --bondif      Bond interface(s) to delete.
                    --member      Bond member interface(s) to delete.
                    --nwif        Eth interface(s) to delete.

```

For example, to delete network interface eth2, run the command: `network --delete --nwif eth2`

Result

Interface delete successful. Please restart networking for the changes to take effect.

network --restart

Description

Restarts the current networking configuration for a DR Series system.

Syntax

```
network --restart
```

Result

```

Shutting down interface eth0:           [ OK ]
Shutting down interface eth1:           [ OK ]
Shutting down interface eth2:           [ OK ]
Shutting down interface eth3:           [ OK ]
Shutting down loopback interface:       [ OK ]
Bringing up loopback interface:         [ OK ]
Bringing up interface bond0:
Determining IP information for bond0... done. [ OK ]
DNS Updated hostname: acme11.storage.local

```

network --setdhcp

Description

Configures the DR Server system to use the dynamic host configuration protocol (DHCP) form of IP addressing.

Syntax

```
network --setdhcp [--bondif <bondN>] [--nwif <ethN>]
    --bondif    Bond interface to create (dhcp).
    --nwif      Eth interface to create (dhcp).
```

Result

Bond device operation successful. Please run 'network --restart' for the changes to take affect.

network --setstatic_ip [--bondif <bondN>] [--nwif <ethN>] --ip <IPv4/IPv6 address> --netmask <netmask> [--gateway <IPv4/IPv6 address>]

Description

Configures the DR Series system to use a static IP address and configures the corresponding netmask (and/or the routing gateway for a DR Series system).

Syntax

```
network --setstatic_ip --ip 10.20.20.20 --netmask 255.255.222.0 --gateway
10.25.20.10
    --bondif    Bond interface to create (static).
    --nwif      Eth interface to create (static).
    --ip        Static IP address to use.
    --netmask   Netmask for the static IP address.
    --gateway   Gateway for routing ('bond0' only).
```

Result

Bond device operation successful. Please run 'network --restart' for the changes to take effect.

network --create_bond

Description

The command allows individual network interfaces to be selected to create a bond. Only non-bonded interfaces can be used to create a bond. When a bond is created, all the individual interfaces chosen for the bond lose their existing settings and their settings are managed by the bond. Interface bonding requires all the network devices in the bond to support the same speed. Interfaces of different devices like twisted pair or fibre can be bonded as long as they support the bonding speed. Currently, only devices which support the same speed can be bonded together. You can create multiple bonds, but each bond must be created individually and the maximum number of bonds cannot exceed the number of devices.

Syntax

```
--create_bond --bondif <bondN>
    [--dhcp]
    [--static]
    --nwif <eth0,eth1,...,ethN>
```

```

[--mode < ALB | 802.3ad>]
[--name < DNS name >]
[--mtu <Supported MTU range 512 - 9000>]
[--ip <IPv4/IPv6 address>]
[--netmask <netmask>]
[--gateway <IPv4/IPv6 address>]
[--restart]

--bondif      Bond interface to create.
--dhcp        Create dhcp interface.
--static      Create static interface.
--nwif        Eth interfaces to bond.
--mode        Bonding mode to use.
--name        DNS name for the interface.
--mtu         Ethernet MTU to use (valid range is 512 - 9000).
--ip          Static IP address to use.
--netmask     Netmask for the static IP address.
--gateway     Gateway for routing.
--restart     Restarts networking after creation.

```

For example, to create bond1 using eth3 and eth4, run the command: `network --create_bond --bondif bond1 --dhcp --nwif eth3,eth4 --mode ALB --restart`

Result

```

Shutting down interface bond0: [ OK ]
Shutting down interface bond1: [ OK ]
Shutting down loopback interface: [ OK ]
Bringing up loopback interface: [ OK ]
Bringing up interface bond0:Determining IP information for bond0... done.
[ OK ]
Bringing up interface bond1:Determining IP information for bond1... done.
[ OK ]
Updating DNS entry for SW-01.local to 10.250.xxx.x ..
Skipping DNS Update 10.250.xxx.x: IP already updated.

```

network --create_eth

Description

The command creates eth interface for the system.

Syntax

```

network --create_eth --nwif <ethN>
    [--dhcp]
    [--static]
    [--name < DNS name >]
    [--mtu <Supported MTU range 512 - 9000>]
    [--ip <IPv4/IPv6 address>]
    [--netmask <netmask>]
    [--restart]

--nwif        Eth interface to create.
--dhcp        Create dhcp interface.
--static      Create static interface.
--name        DNS name for the interface.
--mtu         Ethernet MTU to use (valid range is 512 - 9000).
--ip          Static IP address to use.
--netmask     Netmask for the static IP address.
--restart     Restarts networking after creation.

```

For example, to create eth2, run the command: `network --create_eth --nwif eth2 --dhcp`

Result

Interface operation successful. Please restart networking for the changes to take effect.

network --add_member

Description

Add an interface to an existing bond.

Syntax

```
network --add_member --bondif <bondN>
        --nwif <eth0, eth1, . . . ,ethN>

        --bondif    Bond interface to add to.
        --nwif      Eth interfaces to add.
```

For example, to add eth2 to bond1, run the command: `network --add_member --bondif bond1 --nwif eth2`

Result

Interface add successful. Please restart networking for the changes to take effect.

network --setdns [--suffix <dns suffix>] [--primary <IPv4/IPv6 address>] [--secondary <IPv4/IPv6 address>]

Description

Configures the domain name system (DNS) for a DR Series system, which includes the corresponding DNS suffix and a primary name server IP address (and optionally, a secondary name server IP address).

Syntax

```
network --setdns --suffix storage.local --primary 10.25.20.21 --secondary
10.25.20.25
```

network --setbonding --bondif <bondN> [--mode <ALB | 802.3ad>] [--mtu <supported MTU range 512 - 9000>]

Description


Configures or updates the bonding mode or sets the maximum transmission unit (MTU) number to use for a DR Series system.


Syntax

```
network --bondif bond1 --setbonding --mode ALB --mtu 1750
```

Result


Bond device operation successful. Please run 'network --restart' for the changes to take effect.

 **NOTE:** ALB load balancing does not balance the load properly when the backup servers are on a remote subnet. This is because ALB uses the address resolution protocol (ARP) and ARP updates are subnet-specific. Because of this, ARP broadcasts and updates are not sent across the router. Instead, all traffic is sent to the first interface in the bond. To resolve this ARP-specific issue, make sure that the data source systems reside on the same subnet as the DR Series system.

 **NOTE:** When setting or changing the MTU value, make sure to verify that the Ethernet network switch is capable of supporting an MTU size that is equal to or larger than the value being set. Any mismatch in MTU values between the clients, the Ethernet network switch, and the DR Series system will make it inoperable. The relationship of jumbo frames to MTU is discussed in this topic.

 **NOTE:** When using the DR Series system CLI `--setbonding` and `--mtu` commands, a warning dialog displays with the following message:

```
Incorrectly setting the MTU size will cause the DR4000 to not respond. You will
need to log in to the system console and use the network --setbonding --bondif bond0 --mtu
1500 command
to resolve the issue. Please verify that the switch is enabled and capable of
supporting an MTU size
that is equal to or larger than the value being set. Do you want to continue
(yes/no) ?
```

 **CAUTION:** If the existing bonding setting is changed, the connection to the DR Series system may be lost unless you are sure that the DR Series system can accept this bonding type.

In computer networking, jumbo frames are Ethernet frames with more than 1500 bytes of payload (but in some cases, jumbo frames can carry up to 9000 bytes of payload).

Many Gigabit Ethernet switches and Gigabit Ethernet network interface cards support jumbo frames. Some Fast Ethernet switches and Fast Ethernet network interface cards (NICs) also support jumbo frames.

Some computer manufacturers use 9000 bytes as the conventional limit for jumbo frame sizes. Internet Protocol (IP) subnetworks require that all hosts in a subnet have an identical MTU.

Consequently, interfaces that use a standard frame size and those that use a jumbo frame size should not be in the same subnet. To reduce the chance of interoperability issues, NICs capable of jumbo frames require special configurations to use jumbo frames. For more information, contact your Dell Support representative for assistance.

To verify that the destination system can support a specific frame size you want to attempt, use the following DR Series system CLI commands and specify the frame size in bytes using the following command as an example:

```
network --ping --destination <ip address> --size <number of bytes>
```

network --update

Description

The command updates bonding and individual interface information.

Syntax

```
network --update [--bondif <bondN>]
                  [--nwif <ethN>]
                  [--mode < ALB | 802.3ad>]
                  [--name < DNS name >]
                  [--mtu <Supported MTU range 512 - 9000>]
```

```
--bondif  Bond interface to update.
--nwif    Eth interface to update.
--mode    Bonding mode to use.
```

```
--name      DNS name for the interface.
--mtu      Ethernet MTU to use (valid range is 512 - 9000).
```

For example, to update bond1 to use a different MTU parameter, run the command: `network --update --bondif bond1 --mtu 5000`

Result

WARNING: Incorrectly setting the MTU size will cause the DR appliance to not respond.

Please verify that the switch is enabled and capable of supporting an MTU size that is equal to or larger than the value being set.

Do you want to continue (yes/no) [n]? y

Interface update successful.

network --factory_reset

Description

The command resets bond0 Slave Interfaces according to the option of `auto_bonding_speed`.

Syntax

```
network --factory_reset [--auto_bonding_speed <1G|10G>]
                        --auto_bonding_speed    The speed of the device (1G or 10G)
                                                to bond on restart.
```

Result

WARNING: This will reset network configuration to factory settings and will require a system reboot. Existing configuration will be lost.

Do you want to continue (yes/no) [n]?yes

Reboot the system using the command 'system --reboot' to complete the network factory reset.

network --host

Description

The command manages local hosts.

Syntax

```
network --host [--add] [--ip <IPv4/IPv6 address>] [--name <host name>]
               [--delete] [--ip <IPv4/IPv6 address>] [--name <host name>]

--add        Add local host.
--delete     Delete local host.
--ip         Host IP address to manage.
--name       Host name (FQDN or alias) to manage.
```

network --route

Description

The command helps to manage local routes.

Syntax

```
network --route [--add] [--network <destination networks>] [--netmask
<netmask>] [--gateway <gateway addresses>] [--interface <bondN|ethN|lo>]
[--delete] [--network <destination networks>] [--netmask <netmask>] [--gateway
<gateway addresses>] [--interface <bondN|ethN|lo>]
```

```
--add          Add local route.
--delete       Delete local route.
--network      Destination network.
--netmask      Destination network mask.
--gateway      Gateway to destination network.
--interface    Interface to route through.
```

Result

network --nslookup --destination <ip address | hostname>

Description

Performs a domain name system (DNS) lookup for a DR Series system.

Syntax

```
network --nslookup --destination 10.25.20.15
```

Result

```
10.25.20.15 has name sys-59.storage.local.
```

network --traceroute --destination <ip address | hostname>

Description

Performs a trace route for packets that were sent to a DR Series system.

Syntax

```
network --traceroute --destination 10.25.20.20
```

Result

```
traceroute to 10.15.10.21 (10.15.10.21), 30 hops max, 40 byte packets
 1  10.25.24.1 (10.25.24.1)  0.510 ms  0.654 ms  0.673 ms
 2  10.20.12.16 (10.20.12.16)  7.095 ms  7.564 ms  7.843 ms
 3  10.16.16.2 (10.16.16.2)  1.092 ms  1.097 ms  1.130 ms
 4  10.16.0.9 (10.16.0.9)  1.006 ms  0.980 ms  1.017 ms
 5  10.18.14.97)  6.864 ms  5.703 ms  6.264 ms
 6  10.13.19.5)  7.230 ms  7.230 ms  7.260 ms
 7  10.16.19.6)  8.540 ms  8.624 ms  8.848 ms
 8  10.15.15.11 (10.15.15.11)  8.772 ms  9.032 ms  8.859 ms
 9  10.18.15.18 (10.158.15.18)  10.540 ms  10.674 ms  10.285 ms
10  10.15.0.21 (10.15.0.21)  9.153 ms  9.051 ms  9.216 ms
```

network --ping --destination <ip address | hostname> [--tries <number>] [--size <number>] [--interface <bondN | ethN>]

Description

Pings any target DR Series system by sending five **ICMP ECHO_REQUEST** packets to the specified destination to verify that it can be reached.

Syntax

```
network --ping --destination 10.25.19.5
```

Result

```
PING 10.25.19.5 (10.25.19.5) from 10.20.14.15 bond0: 56(84) bytes of data.
```

```
64 bytes from 10.25.19.5: icmp_seq=1 ttl=64 time=0.039 ms
64 bytes from 10.25.19.5: icmp_seq=2 ttl=64 time=0.049 ms
64 bytes from 10.25.19.5: icmp_seq=3 ttl=64 time=0.041 ms
64 bytes from 10.25.19.5: icmp_seq=4 ttl=64 time=0.041 ms
64 bytes from 10.25.19.5: icmp_seq=5 ttl=64 time=0.049 ms
```

```
--- 10.25.19.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.039/0.043/0.049/0.009 ms
```

Other Command Options

--tries

Specify the number of ping attempts by entering a value using the DR Series system CLI **--tries** command option.

Example

```
network --ping --destination 10.25.19.5 --tries 3
```

```
PING 10.25.19.5 (10.25.19.5) from 10.20.14.15 bond0: 56(84) bytes of data.
```

```
64 bytes from 10.25.19.5: icmp_seq=1 ttl=64 time=0.032 ms
64 bytes from 10.25.19.5: icmp_seq=2 ttl=64 time=0.049 ms
64 bytes from 10.25.19.5: icmp_seq=3 ttl=64 time=0.047 ms
```

```
--- 10.25.19.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 5999ms
rtt min/avg/max/mdev = 0.032/0.043/0.049/0.005 ms
```

--size

Specify a desired ping packet size by entering a value using the DR Series system CLI **--size** command option.

Example

```
network --ping --destination system-69 --size 35
```

```
PING 10.20.19.20 (10.20.19.20) from myDR4000 bond0: 35(63) bytes of data.
```

```
43 bytes from 10.20.19.20: icmp_seq=1 ttl=64 time=0.129 ms
43 bytes from 10.20.19.20: icmp_seq=2 ttl=64 time=0.163 ms
43 bytes from 10.20.19.20: icmp_seq=3 ttl=64 time=0.166 ms
43 bytes from 10.20.19.20: icmp_seq=4 ttl=64 time=0.237 ms
43 bytes from 10.20.19.20: icmp_seq=5 ttl=64 time=0.179 ms
```

```
--- 10.20.19.20.acme.local ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.129/0.174/0.237/0.038 ms
```

--interface

Specify an interface address to use as the source address by entering a value using the DR Series system CLI **--interface** command option.

Example

```
network --ping --destination system-69 --interface bond0
```

network --blink

Description

The command blinks the LED on the specific ethernet device.

Syntax

```
network --blink --nwif <ethN> --time <N>

--nwif    Eth interface to blink.
--time    Blink duration time in seconds (default 10, max 300).
```

For example, to blink the LED for eth3, run the command: `network --blink --nwif eth3 --time 30`

Result

Check the LED on the ethernet card on the back of the system for identification.

network --enable

Description

The command starts the specific ethernet device(s) on restart.

Syntax

```
network --enable [--bondif <bond0,bond1,...,bondN>]
                 [--nwif <eth0,eth1,...,ethN>]

--bondif    Bond interface(s) to delete.
--nwif      Eth interface(s) to dele
```

For example, to enable eth2, run the command: `network --enable --nwif eth2`

Result

Interface device operation successful. Please restart networking for the changes to take effect.

network --disable


Description

The command does not start the specific ethernet device(s) on restart.

Syntax

```
network --disable [--bondif <bond0,bond1,...,bondN>]
                  [--nwif <eth0,eth1,...,ethN>]

--bondif    Bond interface(s) to delete.
--nwif      Eth interface(s) to dele
```

 **NOTE:** You cannot disable eth interfaces which are part of a bond.

For example, to disable eth2, run the command: `network --disable --nwif eth2`


Result

Interface device operation successful. Please restart networking for the changes to take effect.

```
network --troubleshoot [--links] [--gateway] [--ntp] [--dns] [--active_domain] [--nis] [--clients] [--port_mapper] [--network_config] [--show_active <nfs | cifs | ost | rds>] [--interface <bondN | ethN>]
```

Isolates a variety of networking issues that you might encounter while running a DR Series system. When you can isolate a problem or issue to a specific cause, you can better understand and resolve it. The DR Series system CLI **network --troubleshoot** command and its options allow you to perform basic troubleshooting checks on the state of a DR Series system.

Description

 **NOTE:** When entering the **network --troubleshoot** command string, the DR Series system checks and displays the current state for all of the **--troubleshoot** options. To limit the type of network troubleshooting check you want to display, define the command string to a specified check (or checks). For example, using **network --troubleshoot --gateway**, displays the status of the gateway for a DR Series system (for details, see [network --troubleshoot \[--gateway\]](#)).

Syntax

```
network --troubleshoot
```

Result

```
*** Checking link status for each interface
    bond0 : Link detected: yes
    eth0  : Link detected: yes
    eth1  : Link detected: yes
    eth2  : Link detected: yes
    eth3  : Link detected: yes
    lo    : Link detected: yes

*** Getting local IP addresses
bond0 addr:10.25.20.23 Mask:255.255.245.0

*** Getting bond information
Ethernet Channel Bonding Driver: v3.4.0 (October 7, 2008)

Bonding Mode: transmit load balancing
Primary Slave: None
Currently Active Slave: eth0
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0

Slave Interface: eth0
MII Status: up
Link Failure Count: 0
Permanent HW addr: 00:50:56:93:59:7a

Slave Interface: eth1
MII Status: up
Link Failure Count: 0
Permanent HW addr: 00:50:56:93:59:7b
```

Slave Interface: eth2
MII Status: up
Link Failure Count: 0
Permanent HW addr: 00:50:56:93:59:7c

Slave Interface: eth3
MII Status: up
Link Failure Count: 0
Permanent HW addr: 00:50:56:93:59:7d

*** Getting Gateway status
Gateway IP address is 10.25.20.1
Route to the gateway is up and uses bond0 interface.
Pinging gateway 10.25.20.1
Ping successful. No packet loss.
RTT timings min/avg/max/mdev = 0.332/1.612/3.742/1.274 ms

*** Checking NTP configuration
Network time is enabled.
System is configured with following NTP servers:
0.centos.pool.ntp.org
1.centos.pool.ntp.org
2.centos.pool.ntp.org

Checking if NTP servers are reachable...
Pinging 0.centos.pool.ntp.org
Ping successful. No packet loss.
RTT timings min/avg/max/mdev = 75.696/76.042/76.541/0.506 ms
Pinging 1.centos.pool.ntp.org
Ping successful. No packet loss.
RTT timings min/avg/max/mdev = 49.150/50.098/52.292/1.212 ms
Pinging 2.centos.pool.ntp.org
Ping successful. No packet loss.
RTT timings min/avg/max/mdev = 77.854/77.999/78.075/0.085 ms

*** Checking DNS configuration
DNS Suffix: storage.local
Primary Nameserver: 10.25.19.5
Secondary Nameserver: 10.25.19.6
Pinging 10.25.19.5
Ping successful. No packet loss.
RTT timings min/avg/max/mdev = 0.253/0.451/1.123/0.336 ms
Pinging 10.25.19.6
Ping successful. No packet loss.
RTT timings min/avg/max/mdev = 0.239/0.537/1.149/0.326 ms

*** Checking Active Directory configuration
AD configuration: This node has not joined any domain.

*** Checking NIS configuration
NIS domain configuration not found.

*** Checking NFS and CIFS clients configured for various containers
NFS/CIFS clients configured for containers:
-no specific clients-
*** Checking if there is another host with same name
Local system name: acme-01.storage.local
Local system IP: 10.25.20.23
Pinging acme-01.storage.local 3 times
Got IP address as 10.25.20.23
Got IP address as 10.25.20.23
Got IP address as 10.25.20.23
No duplicate hostname found on the network.

```

*** Checking portmapper
portmap (pid 3716) is running
Checking ports currently being used by portmapper
  program vers proto  port
    100000   2   tcp   111  portmapper
    100000   2   udp   111  portmapper

```

network --troubleshoot --gateway --interface <bondN | ethN>

Description

Performs a basic troubleshooting on the current state of the gateway connected to the DR Series system.

Syntax

```
network --troubleshoot --gateway --interface bond0
```

Result

```

*** Getting Gateway status
Gateway IP address is 10.250.240.1
Route to the gateway is up and uses bond0 interface.

Pinging gateway 10.250.240.1
  Ping successful. No packet loss.
  RTT timings min/avg/max/mdev = 0.261/1.907/5.244/1.830 ms

```

network --troubleshoot [--show_active <nfs | cifs | ost | rds>]

Description

Displays the current network activity for NFS, CIFS, OST, or RDS clients that you designate on a DR Series system (this example shows CIFS).

Syntax

```
network --troubleshoot --show_active cifs
```

Result

```

tcp          0          0      10.25.19.10:45      10.25.20.82:52596
ESTABLISHED
tcp          0      0      10.25.19.10:45      10.250.201.68:60163      ESTABLISHED
tcp          0      0      10.25.19.10:45      10.250.208.235:29587      ESTABLISHED
tcp          0      0      10.25.19.10:45      10.250.209.210:13828      ESTABLISHED

```

network --tcpdump [--port <nfs | windows | replication | ost | rds>] [--pkt_size <128 - 32768>] [--file_size <0 - 100>] [--stop] [--host <ip address list>] [--interface <bondN | ethN>]

Intercepts TCP/IP packets being transmitted or received over the network to which the DR Series system is attached. You can filter the packets being collected by using the following options to the DR Series system CLI **network --tcpdump** command:

- **--port** by its type: NFS, CIFS, replication, OST, or RDS port
- **--pkt_size** by the packet size you specify
- **--file_size** by the file size you specify
- **--host** by the IP address (or addresses) that you specify
- **--interface** by the interface that you specify

The tcpdump files are collected on the DR Series system (in /store/tcpdump/), and they can be a valuable resource of information about how your system and network interact. To stop collecting tcpdump files, use the DR Series system CLI **network --tcpdump --stop** command.

network --tcpdump [--pkt_size <128 - 32768>]

Description

Collects TCP/IP packet information based on a specific packet size (for example, 256 Kilobytes or KB).

 **NOTE:** To stop the tcpdump process, use the DR Series system CLI **network --tcpdump --stop** command.

Syntax

```
network --tcpdump --pkt_size 256
```

Result


Successfully started tcpdump, please use "network --tcpdump --stop" to stop.

For more information, see [network --tcpdump \[--port <nfs | windows | replication | ost>\] \[--pkt_size <128 - 32768>\] \[--file_size <0 - 100>\] \[--stop\] \[--host <ip address list>\]](#).

network --tcpdump [--file_size <0 - 100>]

Description

Collects TCP/IP packet information based on a specific file size that you can configure (such as 3 Megabytes or MB).

 **NOTE:** To stop the tcpdump process, use the DR Series system CLI **network --tcpdump --stop** command.

Syntax

```
network --tcpdump --file_size 3
```

Result


Successfully started tcpdump, please use "network --tcpdump --stop" to stop.

For more information, see [network --tcpdump \[--port <nfs | windows | replication | ost>\] \[--pkt_size <128 - 32768>\] \[--file_size <0 - 100>\] \[--stop\] \[--host <ip address list>\]](#).

network --tcpdump [--host <ip address list>]

Description

Collects TCP/IP packet information based on a specific host IP address (for example, 10.10.11.12).


 **NOTE:** To stop the tcpdump process, use the DR Series system CLI **network --tcpdump --stop** command.

Syntax

```
network --tcpdump --host 10.10.11.12
```

Result

Successfully started tcpdump, please use "network --tcpdump --stop" to stop.

 **NOTE:** You can also specify a number of host IP addresses using this command in a comma-delimited format (**--host 10.10.11.12,10.12.12.13,10.10.12.14**).

network --tcpdump [--port <nfs | windows | replication | ost | rds>]

Description

Filters TCP/IP packet information based on a specific port type. In this example, by specifying an OpenStorage Technology (OST) port type using the DR Series system CLI **network --tcpdump --port ost** command.

Syntax

```
network --tcpdump --port ost
```

Result


Successfully started tcpdump, please use "network --tcpdump --stop" to stop.

For more information, see [network --tcpdump \[--port <nfs | windows | replication | ost | rds>\] \[--pkt_size <128 - 32768>\] \[--file_size <0 - 100>\] \[--stop\] \[--host <ip address list>\]](#).

network --iperf_client --server <ip address | hostname> [--port <number>] [--window_size <num bytes [KB/MB]>] [--interval <num seconds>] [--time <num seconds>]

The DR Series system provides the **--iperf** set of DR Series system CLI commands (**--iperf_client** and **--iperf_server**) that let you test network performance between any client and server on the network that you designate. In addition to testing the network performance between these two designated endpoints, this set of **--iperf** commands also let you test if the firewall allows a connection between these two points. You can filter the network performance test by using the following options:

- **--server**, by the IP address or host name that you specify
- **--port**, by the port number that you specify
- **--window_size**, by the number of bytes, Kilobytes or Megabytes (KB/MB), that you specify
- **--interval**, by the number of seconds that you specify
- **--time**, by the number of seconds that you specify

 **NOTE:** There are two conditions you must meet: 1) you must use ports with the **--iperf_client** and **--iperf_server** commands that are not in use by any other system operations (if you do not define specific ports, the **--iperf_client** and **--iperf_server** commands default to port 5001), and 2) these commands must be issued simultaneously.

Description

Tests network performance between a client and server using a designated port (use this command at the same time you use the other **--iperf** command).

```
network --iperf_client --server acme-sw-02 --port 5001 --window_size 7KB --interval 30 --time 60
```


Result

```
-----
Client connecting to acme-sw-02, TCP port 5001
TCP window size: 14.0 KByte (WARNING: requested 7.00 KByte)
-----
[ 6] local 10.20.21.23 port 5812 connected with 10.20.20.3 port 5001
[ ID] Interval      Transfer      Bandwidth
[ 6] 0.0-30.0 sec    193 MBytes   54.0 Mbits/sec
[ 6] 30.0-60.0 sec    205 MBytes   57.4 Mbits/sec
[ 6] 0.0-60.0 sec    398 MBytes   55.7 Mbits/sec
```

network --iperf_server [--port <number>] [--window_size <num bytes [KB/MB>]

The DR Series system provides the **--iperf** set of DR Series system CLI commands (**--iperf_client** and **--iperf_server**) that let you test network performance between any client and server on the network that you designate. In addition to testing the network performance between these two designated endpoints, this set of **--iperf** commands also let you test if the firewall allows a connection between these two points. You can filter the network performance test by using the following options:

- **--port**, by the port number that you specify
- **--window_size**, by the number of bytes, Kilobytes (KB) or Megabytes (MB) that you specify

 **NOTE:** There are two conditions you must meet: 1) you must use ports with the **--iperf_client** and **--iperf_server** commands that are not in use by any other system operations (if you do not define specific ports, the **--iperf_client** and **--iperf_server** commands default to port 5001), and 2) these commands must be issued simultaneously.

Description

Tests network performance between a client and server using a designated port (use this command at the same time you use the other **--iperf** command).

Syntax

```
network --iperf_server --port 5001 --window_size 7KB
```

Result

```
-----  
Server listening on TCP port 5001  
TCP window size: 14.0 KByte (WARNING: requested 7.00 KByte)  
-----  
[ 7] local 10.20.21.23 port 5812 connected with 10.20.20.3 port 5001  
[ ID] Interval      Transfer      Bandwidth  
[ 7] 0.0-60.0 sec   398 MBytes    55.7 Mbits/sec
```

network --help

Description

Displays the list of network-related options that can be used as a reference when using the DR Series system CLI.

Syntax

```
network --help
```

Result

```
network --show [--bondif <bond0,bond1,...,bondN>]  
                [--nwif <eth0,eth1,...,ethN>]  
                [--hosts]  
                [--routes]  
                [--interface <bondN|ethN>]  
  
network --delete [--bondif <bond0,bond1,...,bondN>]  
                [--member <eth0,eth1,...,ethN>]  
                [--nwif <eth0,eth1,...,ethN>]  
  
network --restart  
  
network --setdhcp [--bondif <bondN>]  
                 [--nwif <ethN>]
```

```

network --setstatic_ip [--bondif <bondN>]
    [--nwif <ethN>]
    --ip <IPv4/IPv6 address>
    --netmask <netmask>
    [--gateway <IPv4/IPv6 address>]

network --create_bond --bondif <bondN>
    [--dhcp]
    [--static]
    --nwif <eth0,eth1,...,ethN>
    [--mode < ALB | 802.3ad >]
    [--name < DNS name >]
    [--mtu <Supported MTU range 512 - 9000>]
    [--ip <IPv4/IPv6 address>]
    [--netmask <netmask>]
    [--gateway <IPv4/IPv6 address>]
    [--restart]

network --create_eth --nwif <ethN>
    [--dhcp]
    [--static]
    [--name < DNS name >]
    [--mtu <Supported MTU range 512 - 9000>]
    [--ip <IPv4/IPv6 address>]
    [--netmask <netmask>]
    [--restart]

network --add_member --bondif <bondN>
    --nwif <eth0,eth1,...,ethN>

network --setdns [--suffix <dns suffix>]
    [--primary <IPv4/IPv6 address>]
    [--secondary <IPv4/IPv6 address>]

network --setbonding [--bondif <bondN>]
    [--mode < ALB | 802.3ad >]
    [--mtu <Supported MTU range 512 - 9000>]

network --update [--bondif <bondN>]
    [--nwif <ethN>]
    [--mode < ALB | 802.3ad >]
    [--name < DNS name >]
    [--mtu <Supported MTU range 512 - 9000>]

network --factory_reset [--auto_bonding_speed <1G|10G>]

network --host [--add] [--ip <IPv4/IPv6 address>] [--name <host name>]
    [--delete] [--ip <IPv4/IPv6 address>] [--name <host name>]

network --route [--add] [--network <destination networks>] [--netmask
<netmask>] [--gateway <gateway addresses>] [--interface <bondN|ethN>]
    [--delete] [--network <destination networks>] [--netmask
<netmask>] [--gateway <gateway addresses>] [--interface <bondN|ethN>]

network --nslookup --destination <ip address | hostname>

network --traceroute --destination <ip address | hostname>
    [--interface <bondN|ethN>]

network --ping --destination <ip address | hostname>
    [--tries <number>]
    [--size <number>]
    [--interface <bondN|ethN>]

```

```

network --blink --nwif <ethN>

network --enable [--bondif <bond0,bond1,...,bondN>]
  [--nwif <eth0,eth1,...,ethN>]

network --disable [--bondif <bond0,bond1,...,bondN>]
  [--nwif <eth0,eth1,...,ethN>]

network --troubleshoot [--links]
  [--gateway]
  [--ntp]
  [--dns]
  [--active_domain]
  [--nis]
  [--clients]
  [--port_mapper]
  [--network_config]
  [--show_active <NFS|CIFS|OST|RDS>]
  [--interface <bondN|ethN>]

network --tcpdump [--port <NFS|Windows|Replication|OST|RDA>]
  [--pkt_size <128 - 32768>]
  [--file_size <0 - 100>]
  [--stop]
  [--host <ip address list>]
  [--interface <bondN|ethN>]

network --iperf_client --server <ip address | hostname>
  [--port <number>]
  [--window_size <num bytes [KB/MB]>]
  [--interval <num seconds>]
  [--time <num seconds>]

network --iperf_server [--port <number>]
  [--window_size <num bytes [KB/MB]>]

network --help

network <command> <command-arguments>
<command> can be one of:
  --show          Display network settings.
  --delete        Delete network interfaces(s).
  --restart       Restarts networking.
  --setdhcp      Configures bond interface to use DHCP.
  --setstatic_ip Assigns a static IP address to the bond
interface.
  --create_bond  Create bond interfaces for the machine.
  --create_eth   Create eth interfaces for the machine.
  --add_member   Add an interface to an existing bond.
  --setdns       Configures the Domain Name Servers.
  --setbonding   Updates bonding mode or MTU information.
  --update       Updates bonding and individual interface
information.
  --factory_reset Reset networking to factory configuration.
  --host         Manage local hosts.
  --route        Manage local routes.
  --nslookup     Looks up the IP address/hostname.
  --traceroute   Displays the packets route to network host.
  --ping         Sends ICMP ECHO_REQUEST to destination host.
  --blink        Blink LED on the specific ethernet device.
  --enable       Start the specific ethernet device(s) on
restart.
  --disable      Don't start the specific ethernet device(s)
on restart.

```

```

--troubleshoot    Troubleshoots network issues.
--tcpdump         Capture network traffic.
--iperf_client    Run iperf (Network Performance) in client
mode.
--iperf_server    Run iperf (Network Performance) in server
mode.

```

For command-specific help, please type `network --help <command>`
eg:
`network --help show`

OST


This topic introduces the set of OpenStorage Technology-related DR Series system CLI commands that enable you to perform the following tasks:

- Display command-specific information
- Update the OST user password
- Delete the OST client
- Update the attributes of the OST client
- Limit the bandwidth consumed by OST
- List or clean up partial images

OST Command Usage

This topic introduces the **ost** command usage:

- **ost --show [options]**
- **ost --setpassword**
- **ost --delete_client [options]**
- **ost --update_client [options]**
- **ost --limit --speed --target [options]**
- **ost --partial_images --containerid [options]**
- **ost --help**

 **NOTE:** If you specify a command without supplying the expected value or option, you will be prompted to provide the correct value or option.

ost --show [--config] [--file_history] [--name <name>] [--active_files] [--name <name>] [--clients] [--limits]

Description

Displays the current OpenStorage Technology (OST) configuration information for a DR Series system.

Syntax

```
ost --show [--config]
```

```

[--file_history] [--name <name>]
                 [--active_files] [--name <name>]
                 [--clients]
                 [--limits]

```

```

--config          Displays OST configuration.

```


```

--file_history  Display(s) history of last 10 OST optimized
duplication image file(s).
--name         OST container name.
--active_files Display(s) current OST image files being replicated.
--name         OST container name.
--clients      Displays OST clients.
--limits       Replication speed limits.

```

Result

```
OST Login Entry User      : backup_user
```

 **NOTE:** To display other types of OST configuration information, simply substitute the `--file_history`, `--name <name>`, or `--clients` options in the DR Series system CLI command.

Other Examples

Displays the last 10 replicated files that were processed via the DMA optimized duplication process for an OST container (in this example, the container is `ost-99`.)

```
ost --show --file_history --name ost-99
```

```

Data replication history:
File      /1339632000/ddt_unique_2_thr7
Target IP 10.250.201.49
Target ID 6
Savings   13.46%
Bytes     12485760
Throughput 352581KiB/s
Replicated At: 2012-06-20 09:08:00

```

```


File      /1339632000/ddt_unique_2_thr6
Target IP 10.250.201.49
Target ID 6
Savings   13.10%
Bytes     10585760
Throughput 352581KiB/s
Replicated At: 2012-06-20 09:08:05

```

```

File      /1339545600/ddt_unique
Target IP 10.250.201.49
Target ID 6
Savings   10.50%
Bytes     10885750
Throughput 77101KiB/s
Replicated At: 2012-06-20 09:08:34

```


 **NOTE:** This example intentionally only shows three of the 10 replicated files that were processed.

Displays the OST clients, by running the command: `ost --show --clients`

```

Client      acme-55
Plugin      2.0.0
OS Windows Server 2008 R2 64-bit
Backup Software NetBackup 7.1.2012
Idle Time 00:01:10
Connections 1
Mode Dedupe

```

 **NOTE:** The displayed output when using the DR Series system CLI `ost --show --clients` command could indicate a fourth type of mode value. Depending upon the client, this value would normally display **Auto**, **Dedupe**, or **Passthrough**. However, you could potentially display a mode value of **Mixed**, which indicates that you had changed the mode using the DR Series system CLI while the client is still connected.



NOTE: Be aware that the mode for clients that were connected to the OST media server before configuration changes might be different that what is shown in the displayed output when using the DR Series system CLI **ost --show --clients** command. The configuration changes will be updated and reflect any future connections.

To verify the current state of an OST client, you can check these two sources:

- DR Series system CLI, using the **ost --show --clients** command
- DR Series system GUI, displaying the **Clients** page

These sources display information about the connected and configured clients. For example, when a system is connected to multiple times, these sources show the number of connections to that client and the mode. You can also change the mode from dedupe to the other supported modes. When this is done the displayed mode will change, but any active connections will remain. There are essentially two possible modes: **Dedupe** and **Passthrough**. To verify the current mode of an OST client, you can check these two sources of client statistics:

- DR Series system CLI, using the **stats --container --name** command
- DR Series system GUI, displaying the **Container Statistics** page

In the **Container Statistics** page, click the **Client Statistics** tab (under Connection Type: OST) to display the Client Statistics table. If the Network Savings level in this table displays some savings and the displayed Bytes Ingested value is different from the displayed Bytes Transferred, this indicates that the OST clients are working in the **Dedupe** mode. If not, this indicates that the OST containers are working in the **Passthrough** mode.

ost --setpassword

Description

Updates the current OST user password, when you enter and confirm a new OST password for the **backup_user**.

Syntax

```
ost --setpassword
```

Result

```
Enter new password for backup_user:  
Re-type new password:  
OST password updated successfully.
```

ost --delete_client --name <OST Client Hostname>

Description

The command deletes the OST client and any edits that have been made to its default values. The next time a connection is established between the client and the DR Series system, the default OST connection settings will be used. Deleting an OST client using this CLI command does not affect data already written to the DR Series system.

Syntax

```
ost --delete_client --name acme-99
```

Result

```
Successfully deleted OST client acme-99.
```

ost --update_client --name <OST Client Hostname> --mode <auto | passthrough | dedupe>

Description

Updates the attributes of an OST client (OST client name and mode). The OST client modes are **auto**, **passthrough**, and **dedupe**. If an OST client has four or more CPU cores, it is considered to be dedupe-capable. However, the OST client operating mode depends upon how it is configured in the DR Series system.

- **Auto** — Sets the mode to **dedupe** or **passthrough** as determined by the media server. The mode used is based on how many cores the OST client has and whether it is 32-bit or 64-bit. If the OST client has four or more CPU cores, it will run in the **dedupe** mode. If the OST client has less than four CPU cores, it will run in **passthrough** mode. For details, see the table below.
- **Passthrough** — The OST client passes all data to the DR Series system for dedupe processing. This is also known as “appliance-side dedupe”.
- **Dedupe** — The OST client processes hashing on the data. This is also known as “source-side dedupe” and is the default mode. Keep in mind that the OST client must be dedupe-capable (four or more CPU cores) in order for this mode to be in effect. If the OST client is not dedupe-capable, it will run in **passthrough** mode regardless of its **dedupe** mode setting.


The following table shows the relationship between the configured OST client mode types and the supported client mode based on client architecture type and corresponding number of CPU cores.

Table 2. Supported OST Client Modes and Settings

OST Client Mode Settings	32-Bit OST Client (4 or more CPU Cores)	64-Bit Client (4 or more CPU Cores)	32-Bit OST Client (Less than 4 CPU Cores)	64-Bit OST Client (Less than 4 CPU Cores)
Auto	Passthrough	Dedupe	Passthrough	Passthrough
Dedupe	Not Supported	Supported	Not Supported	Not Supported
Passthrough	Supported	Supported	Supported	Supported

Syntax

```
ost --update_client --name acme-81 --mode dedupe
```

 **NOTE:** You may be able to force writes for OST clients running in the **Passthrough** mode using the DR Series system CLI **mode --dedupe** command. The change in OST client mode is effective on the next backup operation when you are using Symantec NetBackup. (If you are using Symantec Backup Exec, you will need to restart this service for it to recognize that a new mode has been configured.)

Result

```
OST client updated successfully.
```

ost --limit --speed <<num><kbps | mbps | gbps | default> --target <ip address | hostname>

Description

Limits the bandwidth consumed by OST (OpenStorage Technology) for a system you define by IP address or hostname (**--target**), by which you define the speed in kilobytes/second (KBps), megabytes/second (MBps), gigabytes/second (GBps), or an unlimited bandwidth (default).

Syntax

```
ost --limit --speed 10mbps --target acmesys-49
```

Result

Successfully updated bandwidth limit for acmesys-49 to 10 MBps.
Changing traffic control policies ... done.

ost --partial_images --containerid <Container id> [--delete <Partial image path>] [--timeout <> 0]

Description

Lists or cleans up partial images.

- Container id — ID of container.
- Partial image path — OST partial image path to delete.
- Timeout — Maximum timeout (in seconds) to list partial images.

Syntax

```
ost --partial_images --containerid container1
```

ost --help

Description

Displays the list of OpenStorage Technology (OST) ost-related options that can be used as a reference when using the DR Series system CLI.

Syntax

```
ost --help
```

Result

```
ost --show [--config]
           [--file_history] [--name <name>]
           [--active_files] [--name <name>]
           [--clients]
           [--limits]

           ost --setpassword
           ost --delete_client --name <OST Client Hostname>
           ost --update_client --name <OST Client Hostname> --mode <auto|
passthrough|dedupe>
           ost --limit --speed <<num><kbps|mbps|gbps> | default> --target <ip
address | hostname>
           ost --partial_images --containerid <Container id> [--delete <Partial
image path>] [--timeout <> 0]
           ost --help
```

```
ost <command> <command-arguments>
```

<command> can be one of:

--show	Displays command specific information.
--setpassword	Updates the OST user password.
--delete_client	Deletes the OST client.
--update_client	Updates attributes of the OST client.
--limit	Limits bandwidth consumed by OST when replicating over a WAN link.
--partial_images	Lists or cleans up partial images.

For command-specific help, please type `ost --help <command>`

eg:
ost --help show

RDA

The set of RDA commands have the following functions:

- Displays command specific information.
- Updates the Rapid Data Access (RDA) user password.
- Deletes the Rapid Data Access (RDA) client.
- Updates attributes of a Rapid Data Access (RDA) client.
- Limits bandwidth consumed by Rapid Data Access (RDA) when replicating over a WAN link.
- Lists or cleans up partial images.

RDA Command Usage

The following commands are run for RDA:

- **rda --show**
- **rda --setpassword**
- **rda --delete_client**
- **rda --update_client**
- **rda --limit**
- **rda --partial_images --containerid [options]**

rda --show [--config] [--file_history] [--name <name>] [--active_files] [--name <name>] [--clients] [--limits]

Description

The command displays the RDA-specific configurations.

Syntax


```
rda --show      [--config]
                [--file_history] [--name <name>]
                [--active_files] [--name <name>]
                [--clients]
                [--limits]


--config        Displays RDA configuration.
--file_history  Display(s) history of last 10 RDA optimized
                deduplication image file(s).
--name          RDA container name.
--active_files  Display(s) current active RDA image files being
                replicated.
--name          RDA container name.
--clients       Displays RDA clients.
--limits        Replication speed limits.
```

For example, to show the RDA clients, run the command: `rda --show --clients`

Results

RDA Client(s)	Type	Plugin	OS	Backup Software	Last Access	Connection(s)	Mode
BabuK-W2K8-02	RDS	2.1.177	Windows Server 2008 R2	NetVault Backup	Jul 18 05:42:53	1	Passthrough

 **NOTE:** The displayed output when using the `rda --show --clients` command indicates a fourth type of mode value. Depending upon the client, this value equals **Auto**, **Dedupe**, **Passthrough**, or **Mixed**. **Mixed** indicates that you changed the mode while the client is still connected.

 **NOTE:** The mode for clients that are connected to the RDA media server before configuration changes might be different than what is displayed when using the `rda --show --clients` command. The configuration changes are updated to reflect any future connections.

To verify the current state of an RDA client, you can check the two sources:

- DR Series system CLI, using the `rda --show --clients` command
- DR Series system GUI, displaying the **Clients** page

These sources display information about the connected and configured clients. When a system is connected multiple times, these sources show the number of connections to that client and the mode. You can also change the mode from **dedupe** to the other supported modes. When this is done the displayed mode changes, but any active connections remains. There are essentially two possible modes: **Dedupe** and **Passthrough**. To verify the current mode of an RDA client, you can check the two sources of client statistics:

- DR Series system CLI, using the `stats --container --name` command
- DR Series system GUI, displaying the **Container Statistics** page

In the **Container Statistics** page, click the **Client Statistics** tab (under Connection Type: RDS) to display the **Client Statistics** table. If the **Network Savings** level in this table displays some savings and the displayed **Bytes Ingested** value is different from the displayed **Bytes Transferred**, it indicates that the RDA clients are working in the **Dedupe** mode. If not, it indicates that the RDA containers are working in the **Passthrough** mode.

rda --setpassword


Description

The command updates the Rapid Data Access (RDA) user password.

Syntax

```
rda --setpassword
```

For example, to set the `rda` password, run the command: `rda --setpassword`

 **NOTE:** The password has to be between 8 and 12 characters and cannot contain quotes.

Result

```
Enter new password for backup_user:Dell1234
Re-type new password:Dell1234
Rapid Data Access (RDA) password updated successfully.
```

rda --delete_client --name <RDA Client Hostname>

Description

The command deletes the Rapid Data Access (RDA) client and any edits that were made to its default values. The next time a connection is established between the client and the DR Series system, the default RDA connection settings will be used. Deleting an RDA client using this CLI command does not affect data already written to the DR Series system.

Syntax

```
rda --delete_client --name <RDA Client Hostname>
    --name      Host name
```

For example, to delete the client TEST-W2K8-02, run the command: `rda --delete_client --name TEST-W2K8-02`

Result

Rapid Data Access (RDA) client TEST-W2K8-02 deleted successfully.

rda --update_client --name <RDA Client Hostname> --mode <auto| passthrough| dedupe>

Description

The command updates the attributes of a Rapid Data Access (RDA) client. The RDA client modes are **auto**, **passthrough**, and **dedupe**. If a RDA client has four or more CPU cores, it is considered to be dedupe-capable. However, the RDA client operating mode depends upon how it is configured in the DR Series system. For details, see [ost --update_client --name <OST Client Hostname> --mode <auto|passthrough|dedupe>](#).

Syntax

```
rda --update_client --name <RDA Client Hostname> --mode <auto|passthrough|
dedupe>
    --name      Hostname of client
    --mode      RDA modes (auto, dedupe, passthrough)
```

For example, to update the client mode as passthrough for the **BabuK-W2K8-02** client, run the command: `rda --update_client --name BabuK-W2K8-02 --mode passthrough`

Result

Rapid Data Access (RDA) client BabuK-W2K8-02 with mode Pass-through added successfully.

rda --limit --speed <<num><kbps| mbps| gbps> | default> --target <ip address | hostname>

Description

The command limits the bandwidth consumed by RDA when replicating over a WAN link.

Syntax

```
rda --limit --speed <<num><kbps|mbps|gbps> | default> --target <ip address |
hostname>
    --speed      RDA speed limit (eg. 10mbps).
    --target      DR replication target name or IP
address.
```

For example, to limit the speed of testbackup to 4gbps, run the command: `rda --limit --speed 4gbps --target testbackup`

rda --partial_images --containerid <Container id> [--delete <Partial image path>] [--timeout <> 0>]

Description

Lists or cleans up partial images.

- Container id — ID of container.
- Partial image path — RDA partial image path to delete.
- Timeout — Maximum timeout (in seconds) to list partial images.

Syntax

```
rda --partial_images --containerid container1
```

rda --help

Description

Displays the list of RDA-related options that can be used as a reference when using the DR Series system CLI.

Syntax

```
rda --help
```

Result

```
rda --show [--config]
                [--file_history] [--name <name>]
                [--active_files] [--name <name>]
                [--clients]
                [--limits]

rda --setpassword
rda --delete_client --name <RDA Client Hostname>

rda --update_client --name <RDA Client Hostname>
                --mode <auto|passthrough|dedupe>

rda --limit --speed <<num><kbps|mbps|gbps> | default>
                --target <ip address | hostname>

rda --partial_images --containerid <Container id> [--delete <Partial
image path>]
                [--timeout <> 0>]

rda --help

rda <command> <command-arguments>
<command> can be one of:
    --show           Displays command specific information.
    --setpassword    Updates the Rapid Data Access (RDA) user
password.
    --delete_client  Deletes the Rapid Data Access (RDA) client.
    --update_client  Updates attributes of a Rapid Data Access
(RDA) client.
    --limit          Limits bandwidth consumed by Rapid Data
Access (RDA) when replicating over a WAN link.
    --partial_images Lists or cleans up partial images.
```

For command-specific help, please type `rda --help <command>`
eg:
`rda --help show`


Stats

This set of DR Series system CLI commands let you display the current statistics for a DR Series system in the following categories:

- All containers (cumulative): **--system**
- CPU: **--cpu**
- Memory: **--memory**
- Network interfaces: **--network**
- Online data verification: **--datacheck**
- NFS: **--nfs**
- CIFS: **--cifs**
- OST media server: **--ost**
- RDS media server **--rds**
- A specific container: **--container --name**
- Replication: **--replication**
- Cleaner: **--cleaner**
- Clients: **--clients --type**

In addition, this DR Series system CLI command also allows you to reset the following statistic types:

- NFS: **--reset --nfs**
- CIFS: **--reset --cifs**
- OST: **--reset --ost**
- RDS **--reset --rds**
- Data Check: **--reset --datacheck**


 **NOTE:** For information on the **stats --datacheck** commands that are associated with the Data Check feature, see [stats --datacheck](#).

Stats Command Usage

This topic introduces the **stats** command usage:

- **stats --system**
- **stats --cpu**
- **stats --memory**
- **stats --network**
- **stats --datacheck**
- **stats --nfs**
- **stats --cifs**
- **stats --ost**
- **stats --rds**
- **stats --container --name**

- **stats --replication [options]**
- **stats --cleaner**
- **stats --clients [options]**
- **stats --reset [options]**
- **stats --help**

 **NOTE:** If you specify a command without supplying the expected value or option, you will be prompted to provide the correct value or option.

stats --system

Description

Displays the current cumulative system statistics for all of the configured containers on a DR Series system.

Syntax

```
stats --system
```

Result

```
Capacity Used           : 3.0 GiB
Capacity Free          : 7989.0 GiB
Read Throughput        : 0.00 MiB/s
Write Throughput       : 0.00 MiB/s
Current Files          : 11234
Current Bytes          : 6193231169
Post Dedupe Bytes      : 2324390313
Post Compression Bytes : 1409721
Compression Status     : Done
Cleaner Status         : Done
Total Inodes           : 3
Dedupe Savings         : 65.30%
Compression Savings    : 40.24%
Total Savings          : 77.12%
```

stats --cpu

Description

Displays the current cumulative CPU statistics for a DR Series system.

Syntax

```
stats --cpu
```

Result

```
13:00:00 up 9 days, 19:24, 2 users, load average: 1.12, 1.20, 1.18
Cpu(s):  1.4%us,  2.3%sy,  4.0%ni, 99.3%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
```

stats --memory

Description

Displays the current memory statistics in kilobytes (kB) for a DR Series system.

Syntax

```
stats --memory
```

Result

```
MemTotal           : 32425580 kB
MemFree            : 12015828 kB
Buffers            : 46186022 kB
Cached             : 1778860 kB
SwapCached         : 0 kB
Active             : 18802964 kB
Inactive           : 1054936 kB
HighTotal          : 0 kB
HighFree           : 0 kB
LowTotal           : 32425580 kB
LowFree            : 12015828 kB
SwapTotal          : 25165812 kB
SwapFree           : 25165812 kB
Dirty              : 860 kB
Writeback          : 0 kB
AnonPages          : 17617000 kB
Mapped             : 585304 kB
Slab               : 270200 kB
PageTables         : 46228 kB
NFS_Unstable      : 0 kB
Bounce             : 0 kB
CommitLimit       : 55970112 kB
Committed_AS      : 20335148 kB
VmallocTotal      : 34359738367 kB
VmallocUsed       : 393184 kB
VmallocChunk      : 34359343591 kB
HugePages_Total   : 0
HugePages_Free    : 0
HugePages_Rsvd    : 0
Hugepagesize      : 2048 kB
```

stats --network

Description

Displays the current network interfaces (eth0, eth1, eth2, eth3, and bond0) statistics for a DR Series system.

Syntax

```
stats --network
```

Result

```
eth0 Rx Bytes      : 105604787051
eth0 Rx Packets    : 9999546789
eth0 Rx Errors     : 0
eth0 Rx Drops      : 0
eth0 Rx Fifo Errors : 0
eth0 Rx Frame Errors : 0
eth0 Tx Bytes      : 108732530699
eth0 Tx Packets    : 1646686197
eth0 Tx Errors     : 0
eth0 Tx Drops      : 0
eth0 Tx Fifo Errors : 0
eth0 Tx Collision   : 0
eth0 Tx Carrier Error : 0

eth1 Rx Bytes      : 10360478700
eth1 Rx Packets    : 123465437
eth1 Rx Errors     : 0
eth1 Rx Drops      : 0
```

```

eth1 Rx Fifo Errors      : 0
eth1 Rx Frame Errors    : 0
eth1 Tx Bytes           : 10960478703
eth1 Tx Packets         : 195604783
eth1 Tx Errors          : 0
eth1 Tx Drops           : 0
eth1 Tx Fifo Errors     : 0
eth1 Tx Collision       : 0
eth1 Tx Carrier Error   : 0

eth2 Rx Bytes           : 10760478702
eth2 Rx Packets         : 133604783
eth2 Rx Errors          : 0
eth2 Rx Drops           : 0
eth2 Rx Fifo Errors     : 0
eth2 Rx Frame Errors    : 0
eth2 Tx Bytes           : 1235875909
eth2 Tx Packets         : 13578213
eth2 Tx Errors          : 0
eth2 Tx Drops           : 0
eth2 Tx Fifo Errors     : 0
eth2 Tx Collision       : 0
eth2 Tx Carrier Error   : 0
eth3 Rx Bytes           : 1996047831
eth3 Rx Packets         : 133404782
eth3 Rx Errors          : 0
eth3 Rx Drops           : 0
eth3 Rx Fifo Errors     : 0
eth3 Rx Frame Errors    : 0
eth3 Tx Bytes           : 1195604722
eth3 Tx Packets         : 193460478
eth3 Tx Errors          : 0
eth3 Tx Drops           : 0
eth3 Tx Fifo Errors     : 0
eth3 Tx Collision       : 0
eth3 Tx Carrier Error   : 0


bond0 Rx Bytes          : 105604787051
bond0 Rx Packets        : 135791120
bond0 Rx Errors         : 0
bond0 Rx Drops          : 0
bond0 Rx Fifo Errors    : 0
bond0 Rx Frame Errors   : 0
bond0 Tx Bytes          : 108732530699
bond0 Tx Packets        : 1646686197
bond0 Tx Errors         : 0
bond0 Tx Drops          : 0
bond0 Tx Fifo Errors    : 0
bond0 Tx Collision      : 0
bond0 Tx Carrier Error  : 0

```

stats --datacheck

Description

Displays the current set of datacheck statistics on a DR Series system.

 **NOTE:** The Progress field in the statistics can indicate one of three values: **Waiting**, **Running**, and **Idle**.

- **Waiting:** Data Check is in this state because another operation is now running.
- **Running:** Data Check is in this state when running the scans.
- **Idle:** Data Check is in this state waiting for the next opportunity to run the Data Check scans.

The following example shows the status of active DR Series system operations in response to the **stats --datacheck** command on a DR Series system when Data Check is enabled.

Syntax

```
stats --datacheck
```

Result

```
Data Check : Enabled -
namespace,blockmap,throttle:75%
Progress : Idle
Active Writes : No
Active System Operations : No
Total Detected Errors : 0
Last Complete Namespace Scan : 2012-02-02 17:48:18
Last Complete Blockmap Scan : 2012-02-02 16:33:08
Namespace Scans Completed : 183
Namespace Scan Entries : 6
Namespace Scan Errors : 0
Namespace Scan Start Time : 2012-02-02 17:43:08
Namespace Scan Progress : 100.00%
Blockmap Scans Completed : 8
Blockmap Scan Entries : 3
Blockmap Scan Errors : 0
Blockmap Scan Start Time : 2012-02-02 16:33:06
Blockmap Scan Progress : 100.00%
```

Other Examples

This example shows the output from the **stats --datacheck** command used on a DR Series system when Data Check is disabled.

```
stats --datacheck

Online Data Verification : Disabled
Progress : Disabled
Active Writes : No
Active System Operations : No
Total Detected Errors : 0
Last Complete Namespace Scan : 2012-01-24 15:50:10
Last Complete Blockmap Scan : 2012-01-24 15:55:59
```

stats --nfs

Description

Displays the current NFS statistics for a DR Series system.

Syntax

```
stats --nfs
```

Result

```
NFS Per Op Statistics
Procedure      Calls      Avg(us)      Max(us)      Errors
-----
NULL           94         277          4172         0
GETATTR       52552      19946        19905631     0
SETATTR       1031       629602       166232015    0
LOOKUP        2227       18897        1918992      1673
ACCESS        26221      543          416780       0
READLINK      0          0            0            0
```

READ	5302595	240217	856398852	1
WRITE	12872	188647	6853027	0
CREATE	1031	917970	23587115	0
MKDIR	0	0	0	0
SYMLINK	0	0	0	0
MKNOD	0	0	0	0
REMOVE	44996	155136	6458023	0
RMDIR	0	0	0	0
RENAME	0	0	0	0
LINK	0	0	0	0
READDIR	0	0	0	0
READDIRPLUS	85566	30674	28308673	0
FSSTAT	30	321247	1133437	0
FSINFO	104	55279	2402344	0
PATHCONF	52	30217	1466732	0
COMMIT	1031	102190	5506293	0
XWRITE	676364	0	0	0

stats --cifs

Description

Displays the current CIFS statistics for a DR Series system.

Syntax

```
stats --cifs
```

Result

CIFS Per Op Statistics				
Procedure	Calls	Avg (us)	Max (us)	Errors

CONNECT	240	536311	1545946	0
DISCONNECT	214	1979	13127	0
CREATE	271	147101	1170580	0
OPEN	0	0	0	0
CLOSE	0	0	0	0
PREAD	1223941	6167	856679104	0
IOV_PREAD	0	0	0	0
PWRITE	4629174	26376	529148935	0
IOV_PWRITE	0	0	0	0
FTRUNCATE	0	0	0	0
LSTAT	0	0	0	0
FCNTL	0	0	0	0
CANCEL	0	0	0	0
FSTAT	548246	325	7495992	0
FSTAT_BY_PATH	0	0	0	0
READDIR	5064	106833	13550728	0
OPENDIR	2478	160	3671	0
OPENDIR_BY_PATH	0	0	0	0
CLOSEDIR	2477	22	1434	0
MKDIR	0	0	0	0
MKDIR_BY_PATH	0	0	0	0
REMOVE	0	0	0	0
REMOVE_BY_PATH	18026	90875	4900538	0
RENAME	0	0	0	0
RENAME_BY_PATH	0	0	0	0
RMDIR	0	0	0	0
RMDIR_BY_PATH	0	0	0	0
FCHMOD	0	0	0	0
FCHMOD_BY_PATH	0	0	0	0
FCHOWN	0	0	0	0
FCHOWN_BY_PATH	0	0	0	0

FSYNC	226	16257	561552	0
STATVFS	0	0	0	0
STATVFS_BY_PATH	0	0	0	0
UTIME	0	0	0	0
UTIME_BY_PATH	0	0	0	0
MKFIFO	0	0	0	0
MKNOD	0	0	0	0
READLINK	0	0	0	0
READLINK_BY_PATH	0	0	0	0
LINK	0	0	0	0
LINK_BY_PATH	0	0	0	0
SYMLINK	0	0	0	0
SYMLINK_BY_PATH	0	0	0	0
FLOCK	0	0	0	0
SETXATTR	271	87332	565006	0
SETXATTR_BY_PATH	512	95902	896865	0
GETXATTR	922	21916	687777	0
GETXATTR_BY_PATH	354219	18363	3902905	0
LISTXATTR	676	25103	551572	0
LISTXATTR_BY_PATH	261591	9222	4276854	0
REMOVEXATTR	0	0	0	0
REMOVEXATTR_BY_PATH	0	0	0	0
FD_FROM_PATH	610645	1609	856224591	0
GET_REAL_FILENAME	1358	17105	860143	0
XWRITE	0	0	0	0

CIFS I/O Statistics

Procedure	Avg (bytes)	Max (bytes)	Min (bytes)
READ	52429	61440	61440
WRITE	65536	65536	65536
XWRITE	0	0	0

stats --ost

Description

Displays the current OpenStorage Technology (OST) statistics categories for a DR Series system.

Syntax

```
stats --ost
```

Result

OST Server Statistics

Procedure	Errors	Calls	Avg (us)	Max (us)
GET_AUTH		250	120	
250	0			
OPEN_SERVER		178	84	
178	0			
CLOSE_SERVER		110	55	
110	0			
CREATE_FILE		147	73	
147	0			
OPEN_FILE		250	120	
250	0			
CLOSE_FILE		246	123	246
UNLINK_FILE		310	155	310
0				
WRITE_FILE		0	0	
				0

0	0				
READ_FILE	0	0	0		
0	0				
REPLICATE_FILE	0		0		
0	0				
LIST_LSU	399		120		
399	0				
OPENDIR	257		129		
257	0				
CLOSEDIR	1110		368		
1110	0				
READDIR	490		289		
490	0				
SET_LSU_INFO	167		85		
167	0				
GET_LSU_INFO	175		95		
175	0				
REPL_SVR_SETUP	415		235	415	0
GET_IMAGE_INFO	678		346	678	0

stats --rds

Description

Displays statistics for RDS server.

Syntax

```
stats --rds
```

Result

Procedure	Calls	Avg(us)	Max(us)	Errors
GET_AUTH	1	0	0	0
OPEN_SERVER	1	0	0	0
CLOSE_SERVER	0	0	0	0
CREATE_FILE	0	0	0	0
OPEN_FILE	34600	0	35	0
CLOSE_FILE	34600	0	25	0
UNLINK_FILE	0	0	0	0
WRITE_FILE	1	0	0	0
READ_FILE	69198	0	0	0
REPLICATE_FILE	0	0	0	0
LIST_LSU	1	26	26	0
OPENDIR	0	0	0	0
CLOSEDIR	0	0	0	0
READDIR	0	0	0	0
SET_LSU_INFO	0	0	0	0
GET_LSU_INFO	2	0	0	0
REPL_SVR_SETUP	0	0	0	0
GET_IMAGE_INFO	0	0	0	0
MKDIR	0	0	0	0
RMDIR	0	0	0	0
RENAME	0	0	0	0
ACCESS	34604	0	0	0
GETSCID	34600	0	1	0

stats --container --name <name>

Description

Displays the current statistics for a specific container in a DR Series system that you define by name using the DR Series system CLI `--name <name>` command.

Syntax

```
stats --container --name backupsys-60_replicate
```

Result

```
Container Name      : backupsys-60_replicate
Container ID        : 3
Total Inodes        : 1
Read Throughput     : 3.91 MiB/s
Write Throughput    : 3.45 MiB/s
Current Files       : 109931
Current Bytes       : 6193231169
Cleaner Status      : Done
```

stats --replication [--name <name>]

Description

Displays the current replication statistics for all containers in a DR Series system or for a specific container in a DR Series system that you define using the DR Series system CLI `--name <name>` command.

Syntax

```
stats --replication --name backup-acme-60_replicate
```

Result

```
Container Name      :
backup_acme-60_1234567
Replication Target Container      : backup
Replication Target System        : 10.25.19.16
Peer Status                    : Stopped
Replication State                : INSYNC
Schedule Status                 : Outside window
(starts in 0 days 10 hours 6 min 0 sec
Replication Average Throughput    : 4154 KiB/s
Replication Maximum Throughput    : 15710 KiB/s
Network Average Throughput        : 3759 KiB/s
Network Maximum Throughput        : 14999 KiB/s
Network Bytes Sent                : 154.45 MiB
Network Savings                  : 56.60 %
Last INSYNC Time                 : 2012-06-20 09:11:42
Estimated Time To Sync           : 0 days 7 hours 3 minutes 19
seconds
```

Data replication history

```
File : /vargen/source/Office_Docs/Email/Outlook/3244.flate, 44.70%, 88773
bytes, 1305 KB/s, replicated at : 2012-06-19 11:47:03
```

```
File : /vargen/source/status/DEV/August11/dev-status.doc, 100.00%, 86200 bytes,
4310 KB/s, replicated at : 2012-06-19 11:47:03
```

```
File : /vargen/source/MKT/whitepaper/eng/324.tar.gz, 0.00%, 5182 bytes, 259
```

KB/s, replicated at : 2012-06-19 11:47:03

File : /vargen/source/acctspay/status/Sept11/3242.tar.gz, 65.23%, 94616 bytes, 1456 KB/s, replicated at : 2012-06-19 11:47:03

File : /vargen/source/revenue/Q311/interna/324.xls, 0.00%, 5152 bytes, 286 KB/s, replicated at : 2012-06-19 11:47:03

File : /vargen/source/projects/Q411/europe/3244.tar.gz, 62.94%, 8828 bytes, 1193 KB/s, replicated at : 2012-06-19 11:47:03

stats --cleaner

The Cleaner is an asynchronous process in the DR Series system that reclaims disk storage space by reclaiming space that previously contained unreferenced datastore files.

The Cleaner process operates in two distinct phases:

- Information collection
- Space reclamation

Description

Displays the current Cleaner statistics for a DR Series system.

Syntax

```
stats --cleaner
```

Result

```
Last Run Files Processed           : 100
Last Run Bytes Processed           : 100
Last Run Bytes Reclaimed           : 24
Last Run Start Time                : 06/17/12 15:29:31
Last Run End Time                  : 06/17/12 15:29:52
Last Run Time To Completion(s)     : 1.00
Current Run Start Time             : 06/17/12 15:30:51
Current Run Files Processed        : 10
Current Run Bytes Processed        : 10
Current Run Bytes Reclaimed        : 3
Current Run Phase 1 Start Time     : 06/17/12 15:30:52
Current Run Phase 1 Records Processed : 4
Current Run Phase 1 End Time       : 06/17/12 15:30:57
Current Run Phase 2 Start Time     : 06/17/12 15:30:59
Current Run Phase 2 Records Processed : 3
Current Run Phase 2 End Time       : 06/17/12 15:31:12
Current Run Phase 3 Start Time     : 06/17/12 15:31:15
Current Run Phase 3 Records Processed : 2
Current Run Phase 3 End Time       : 06/17/12 15:31:22
Current Run Phase 4 Start Time     : 06/17/12 15:31:32
Current Run Phase 4 Records Processed : 1
Current Run Phase 4 End Time       : 06/17/12 15:31:35
```

stats --clients [--type <nfs | cifs | ost | rds>]

Description

Displays the current NFS, CIFS, OST, or RDS clients that are configured on the DR Series system.

Syntax

```
stats --clients
```

Result

No NFS client(s) are connected.

No CIFS client(s) are connected.

RDS Client(s)	OS	Mode	Backup	Type	Plugin	Last Access
Connection(s)			Software			
BabuK-W2K8-02	2008 R2	NetVault 9.20 Build 12		RDS	2.1.201	Windows Server
1		Passthrough			Aug 13 07:53:26	
R720xd-Netvault				RDS	--	--
--			--			--
0		Default				

To filter the list of clients to display a specific client type (for example, NFS clients) on a DR Series system, use the DR Series system CLI **--type** command:

```
stats --clients --type nfs
No NFS clients connected.
```

 **NOTE:** For OST clients, the value under **Connections** is **0** (zero) when the connection is configured (but it is not in use), and **1** when the connection is in use.

stats --reset [--nfs] [--cifs] [--ost] [--rds] [--datacheck]

Description

Resets the current NFS, CIFS, OST, RDS, or Data Check statistics for a DR Series system. The following example shows **--nfs**; to reset another statistic type, just replace that option type in the DR Series system CLI command.

Syntax

```
stats --reset -nfs
```

Result

Successfully reset NFS stats.

stats --reset --datacheck

Description

Resets the current set of Data Check statistics on a DR Series system.

Syntax

```
stats --reset --datacheck
```

Result

Datacheck statistics reset successfully.

stats --help

Description

Displays the list of all stats-related options that can be used as a reference when using the DR Series system CLI.

Syntax

```
stats --help
```

Result

Usage:

```
stats --system
stats --cpu
stats --memory
stats --network
stats --datacheck
stats --nfs
stats --cifs
stats --ost
stats --rds
stats --container --name <name>

stats --replication [--name <name>]

stats --cleaner

stats --clients [--type <nfs | cifs | ost | rds>]

stats --reset [--nfs]
                [--cifs]
                [--ost]
                [--rds]
                [--datacheck]

stats --help
```

```
stats <command> <command-arguments>
```

<command> can be one of:

--system	Displays cumulative statistics for all containers.
--cpu	Displays CPU statistics.
--memory	Displays statistics for memory.
--network	Displays statistics for network interfaces.
--datacheck	Displays statistics for online data verification.
--nfs	Displays statistics for NFS.
--cifs	Displays statistics for CIFS.
--ost	Displays statistics for OST server.
--rds	Displays statistics for RDS server.
--container	Displays statistics for a specific container.
--replication	Displays statistics for replication.
--cleaner	Displays statistics for cleaner.
--clients	Displays client information.
--reset	Resets statistics.

For command-specific help, please type `stats --help <command>`

For example:

```
stats --help reset
```


stats --datacheck

This set of DR Series system CLI commands allow you to display the current Data Check statistics gathered by the system, reset the Data Check statistics for the system, and display the statistic-based Data Check help-related options. For more information, see [Stats --Datacheck Command Usage](#).

stats --datacheck Command Usage

This topic introduces the **stats --datacheck** command usage:

- **stats --datacheck**
- **stats --reset --datacheck**
- **stats --help datacheck**

 **NOTE:** If you specify a command without supplying the expected value or option, you will be prompted to provide the correct value or option.

stats --help datacheck

Description

Displays the list of stats command-based Data Check options that can be used as a reference when using the DR Series system CLI.

Syntax

```
stats --help datacheck
--datacheck - Displays statistics for online data verification.
```

Result

Usage:
`stats --datacheck`

System

This DR Series system CLI command and its options allow you to perform the following types of system-related tasks:

- Displaying the current system configuration
- Initializing, rebooting, or shutting down the DR Series system
- Upgrading the DR Series system software
- Configuring the compression type to use on the stored data
- Setting the system date and time
- Setting the network time protocol (NTP)
- Updating the login password
- Enabling or disabling telnet access
- Enables or disables marker detection status


 **NOTE:** For information on the **system --datacheck** commands that are associated with the Data Check feature, see [system --datacheck](#).

System Command Usage

This topic introduces the **system** command usage:

- **system --show [options]**
- **system --reboot**
- **system --shutdown**

- **system --upgrade**
- **system --license [options]**
- **system --setname --name**
- **system --setcompression [options]**
- **system --setdate [options]**
- **system --setntp [options]**
- **system --setlogin**
- **system --telnet [options]**
- **system --datacheck [options]**
- **system --marker [options]**
- **system --add_storage --enclosure**
- **system --storage [options]**
- **system --mgmt_traffic**
- **system --backup_traffic**
- **system --replication_traffic**
- **system --opdup_traffic**

 **NOTE:** If you specify a command without supplying the expected value or option, you will be prompted to provide the correct value or option.

system --show [--config]

Description

Displays the current system configuration summary for a DR Series system.

For specific sources of additional system configuration information, see the following **system --show** command options:

- **--hardware**
- **--storage [--type <boot |internal |external>] [--service_tag <service tag>]**
- **[--license] [--verbose]**
- **[--ntp]**
- **--version**
- **--timezones [Region]**
- **--upgradefile**
- **--upgradehistory**
- **[--marker]**
- **[--replication_traffic]**
- **[--opdup_traffic]**
- **[--backup_traffic]**
- **[--mgmt_traffic]**

Syntax

```
system --show --config
```

Result

```
System Name           : acme-55
Current Time          : Wed Oct 16 14:00:32 2013 PDT
Service Tag           : IVQXSS2
Product Name          : Dell DR4100
```

```


BIOS Version           : 2.0.18
Version                : 3.0.0.1.47757
Build                  : 47757
Telnet State           : Disabled
Compression Level      : Balanced
Time Zone              : US/Pacific
Data Check             : Enabled - namespace,blockmap,throttle:50%
Marker Detection       : Enabled
IP Addr                : 10.25.242.12
MAC Addr               : 00:1B:21:C5:92:82
System State           : Operational Mode
Reason                 : Filesystem is fully operational for I/O.
Diagnostics Collector : RUNNING Oct 16 12:14:23
Configuration Server   : RUNNING Oct 16 14:28:19
Filesystem Server      : RUNNING Oct 16 14:28:22
Windows Access Server  : RUNNING Oct 16 14:28:19
HTTP Server            : RUNNING Oct 16 21:01:07
Hardware Health Monitor : RUNNING Oct 16 12:14:24
Windows Active Directory Client : RUNNING Oct 16 12:18:29
Filesystem Checker     : STOPPED

```

system --show [--hardware]

Description

Displays the current DR Series system hardware status for the system hardware components.

 **NOTE:** Due to length, the following example only shows a partial listing of the DR Series system hardware status that is displayed when using this DR Series system CLI command.

Syntax

```
system --show --hardware
```

Result

Component	Type	Signature	Health	PD_Count
Storage Controller	PERC H700	HDB ST00	optimal	14
Storage Controller	PERC H800	HDB ST01	optimal	48

Component	Signature	State	Health	Raid_Level	Agg_Status	PD_Count	Name
Virtual Disk	HDB VD00	ready	optimal	1	1	2	
Virtual Disk 0							
Virtual Disk	HDB VD01	ready	optimal	6	1	11	
DATAVol							

Component	Signature	State	Spare_Config	Spare_State	Health	Slot	Serial	Alert
Size	Type							
Phys Disk	HDB PD00	online	global	no	optimal	0	9WK4ZJ82	no
1 TB	Internal							

system --show [--storage] [--type <boot | internal | external>] [--service_tag <service tag>]

Description

Displays current configuration information about the storage types installed in a DR Series system.

Syntax

```
system --show --storage --type external --service_tag HCM0PT3
```

Result

Component	Signature	State	Health	Raid_Level	Agg_Status
PD_Count	Name				
Virtual Disk	HDB VD02	background_init	optimal	6	1
16	ENCLVol_1				

Component	Signature	State	Spare_Config	Spare_State	Health	Slot	Serial
Alert	Size Type						
Phys Disk	HDB PD14	ready	dedicated	no	optimal	0	Z1P1Z5AG
no	2 TB Encl - 1						
Phys Disk	HDB PD15	ready	no	no	optimal	1	Z1P1YVFW
no	2 TB Encl - 1						
Phys Disk	HDB PD16	ready	no	no	optimal	2	Z1P27A94
no	2 TB Encl - 1						
Phys Disk	HDB PD17	ready	no	no	optimal	3	Z1P229LJ
no	2 TB Encl - 1						
Phys Disk	HDB PD18	ready	no	no	optimal	4	Z1P26VKC
no	2 TB Encl - 1						
Phys Disk	HDB PD19	ready	no	no	optimal	5	Z1P26SLK
no	2 TB Encl - 1						
Phys Disk	HDB PD20	ready	no	no	optimal	6	Z1P26QBM
no	2 TB Encl - 1						
Phys Disk	HDB PD21	ready	no	no	optimal	7	Z1P1R6T3
no	2 TB Encl - 1						
Phys Disk	HDB PD22	ready	no	no	optimal	8	Z1P26TK6
no	2 TB Encl - 1						
Phys Disk	HDB PD23	ready	no	no	optimal	9	Z1P26MZ8
no	2 TB Encl - 1						
Phys Disk	HDB PD24	ready	no	no	optimal	10	Z1P27C4S
no	2 TB Encl - 1						
Phys Disk	HDB PD25	ready	no	no	optimal	11	Z1P1WR0F
no	2 TB Encl - 1						

Component	Signature	Health	Name	NexusId
EMM	HDB EM00	optimal	"EMM 0"	"\\1\\0\\0\\0"
EMM	HDB EM01	optimal	"EMM 1"	"\\1\\0\\0\\1"

Component	Signature	Health	Name	Vendor
PartNumber				
Power Supply	HDB EP00	optimal	"Power Supply 1"	"DELL"
"ONFCG1A02"				
Power Supply	HDB EP01	optimal	"Power Supply 2"	"DELL"
"ONFCG1A02"				

Component	Signature	Health	Temp_Reading
Name	Vendor		
Temperature Probe	HDB ET00	optimal	27.0
Probe 0"	"DELL"		
Temperature Probe	HDB ET01	optimal	29.0
Probe 1"	"DELL"		
Temperature Probe	HDB ET02	optimal	21.0
Probe 2"	"DELL"		
Temperature Probe	HDB ET03	optimal	21.0
Probe 3"	"DELL"		

Component	Signature	Health	Speed	Name	Vendor
Fan	HDB EF00	optimal	0	"ONFCG1A02"	"DELL"
Fan	HDB EF01	optimal	0	"ONFCG1A02"	"DELL"
Fan	HDB EF02	optimal	0	"ONFCG1A02"	"DELL"
Fan	HDB EF03	optimal	0	"ONFCG1A02"	"DELL"

system --show [--storage]

Description

Displays the service tag, size, configuration state, RAID level, the percentage used, and the state of the storage type (or types) installed on a DR Series system.

Syntax

```
system --show --storage
```

Result

Type	Service Tag	RawSize	Configured	RAIDLevel	Used	State
Boot	16TGJTR	278.88 GB	Yes	1	--	ready
Internal	16TGJTR	8.18 TB	Yes	6	2.69%	ready
Enclosure-1	DCGTXR1	8.18 TB	No	--	--	ready

For more information about a system storage, see [system --add_storage --enclosure <service tag>](#) and [system --show \[--storage\] \[--type <boot | internal | external>\] \[--service_tag <service tag>\]](#).

system --show [--license] [--verbose]

Description


Displays the summary license status (using the **system --show --license** command) or the detailed license status (using the **system --show --license --verbose** command) for the current data storage expansion shelves (enclosures) installed in a DR Series system. For more information on validating or adding licenses for data storage expansion shelves, see [system --license \[--validate\] \[--add\]](#).

Syntax

```
system --show --license
```

Result

ID	Description	Status
1	1 Storage Enclosure	Enabled

 **NOTE:** To display a more detailed license status, use the following DR Series system CLI command:

```
system --show --license --verbose
Feature ID                : 1
Description                : 1 Storage Enclosure
Status                    : Enabled
Entitlementment ID        : XKE00000003387477
Start Date                :
End Date                  :
Is Eval                   : No
In Use                    : No
```

system --show [--ntp]

Description

Displays the current NTP service configuration for the DR Series system.

Syntax

```
system --show --ntp
```

Result

```
NTPD Service is           : UP
Server 1                  : 0.centos.pool.ntp.org
Server 2                  : 1.centos.pool.ntp.org
Server 3                  : 2.centos.pool.ntp.org
```

system --show [--version]

Description

Displays the currently installed version of the DR Series system software, and the date and time in which it was installed.

Syntax

```
system --show --version
```

Result

```
Version      : 2.0.0.12345 Sat Oct 20 14:07:41 PDT 2012
```

system --show [--timezones [Region]]

Description

Displays the entire set of time zones that can be selected for a DR Series system, and also displays the time zones that can be selected in a specific region.


Syntax

```
system --show --timezones
```

Result

Following are the time zone regions.

Africa	America	Antarctica	Arctic
Asia	Atlantic	Australia	
Brazil	CET	CST6CDT	Canada
Chile	Cuba		EET
EST		EST5EDT	Egypt
Eire		Etc	Europe
GB		GB-Eire	GMT
+0	GMT0	Greenwich	HST
Hongkong	Iceland	Indian	
Iran	Israel	Jamaica	Japan
Kwajalein	Libya	MET	
MST		MST7MDT	Mexico
NZ		NZ-CHAT	Navajo
PRC		PST8PDT	Pacific
Portugal	ROC		Poland
Singapore	Turkey	UCT	ROK
UTC		Universal	US
WET		Zulu	W-SU

 **NOTE:** To display the time zones that can be selected in a specific region, use the following command:

```
system --show --timezones Chile
Following are the time zones in Chile region:
Continental
Easter Island
```

system --show [--upgradefile]

Description

Displays the current version of the DR Series system software upgrade file that resides on the system appliance.

Syntax

```
system --show --upgradefile
```

Result

```
Version                : 2.0.0.0.47757
MD5 Checksum           : 14caa61e2506818cded12aa2a6f12ea5
```

system --show [--upgradehistory]

Description

Displays the upgrade history for a DR Series system.

Syntax

```
system --show --upgradehistory
```

Result

```
Update Manager started at      : 2012/10/5 16:24:16
Version                        : 1.1.1.0
Update Manager started at      : 2012/10/05 16:26:33
Version                        : 1.1.1.0
Update status                   : SUCCESS, REBOOT REQUIRED
Update Manager finished at     : 2012/10/05 18:01:22
Update Manager started at      : 2012/10/08 18:11:39
Update Manager started at      : 2012/10/08 18:12:01
Version                        : 2.0.0.0.1356
Update status                   : SUCCESS, REBOOT REQUIRED
```

system --show [--marker]

Description

Displays the current state of marker detection in a DR Series system.

Syntax

```
system --show --marker
```

Result

```
Marker Detection      : Enabled
```

system --show [--replication_traffic]

Description

Displays configured dedicated replication network interface(s).

Syntax

```
system --show --replication_traffic
```

Result

```
Application:                replication
Application Interface(bond0): 10.250.xxx.x
```

system --show [--opdup_traffic]

Description

Displays the configured dedicated optimized copy network interface(s).

Syntax

```
system --show --opdup_traffic
```

Result

```
Application:                opdup_incoming
Application Interface(bond1): 10.250.xxx.x
```

system --show [--backup_traffic]

Description

Displays the configured dedicated backup network interface(s).

Syntax

```
system --show --backup_traffic
```

Result

```
Application:                OST
Application Interface(bond1): 10.250.xxx.x
```

system --show [--mgmt_traffic]

Description

Displays the configured dedicated appliance management network interface(s).

Syntax

```
system --show --mgmt_traffic
```

Result

```
Application:                webserver
Application Interface(bond3): 10.250.xxx.x
```

system --reboot

Description

Reboots a DR Series system when you provide the required "administrator" password for the system.

Syntax

```
system --reboot
```


Result

```
Please enter administrator password:
Broadcast message from root (pts/0) (Wed Jun 20 11:00:58 2012):
The system is going down for reboot NOW!
```

system --shutdown

Description

Shuts down a DR Series system when you use this command and provide the required password.

 **CAUTION:** The `system --shutdown` command powers off the appliance on which the DR Series system software is installed. Once the appliance is in a powered off state, you may only be able to power on the appliance in two ways: at its physical location, or by using an iDRAC connection on the network.

Syntax

```
system --shutdown
```

Result

```
Please enter administrator password:
Broadcast message from root (pts/0) (Wed Oct 20 11:00:58 2012):
The system is being shutdown NOW!
```


system --upgrade


Description

Upgrades the version of the DR Series system software installed on a supported DR Series hardware appliance.


Syntax

```
system --upgrade
```

 **NOTE:** To obtain the latest DR Series system upgrade image, navigate to the Dell Support website (dell.com/support), enter your service tag or select your product, and download the latest DR Series system software upgrade image file to the local system using WinSCP.

 **NOTE:** Prior to performing a DR Series system CLI-based upgrade, make sure to download the DR Series system upgrade image. To initiate a DR Series system software upgrade for Windows users using the DR Series system CLI, the system software upgrade image file (in tar.gz format) is validated by the DR Series system, renamed to `DRSeries_payload.tar.gz`, and transferred to a directory/store location known to the DR Series system.

When you use the DR Series system CLI `system --upgrade` command, the DR Series system looks in this known directory/store location for the `DRSeries_payload.tar.gz` file, and starts the system software upgrade process.

 **NOTE:** If the SSH session is lost for any reason during the upgrade process, this loss terminates the SSH session and also terminates the upgrade process that was running. If this SSH session loss occurs during an upgrade process and results in a terminated session, you should reboot the DR Series system and retry the system software upgrade process.


system --license [--validate] [--add]

Description

Validates and installs the license for the external data storage you can add using the expansion shelf enclosures to the base DR Series system. The expansion shelf licenses are based on the size of the expansion shelves; for details on expansion shelves, see [DR Series System Drive and System Capacities](#). There are two ways that expansion shelf licenses can be purchased: point of sale (POS) and after point of sale (APOS).

- POS licenses are those ordered from the factory with the DR Series system hardware appliance and the expansion shelf enclosures.


- APOS licenses are those ordered later separately from Dell for new expansion shelves or for existing Dell MD1200 storage arrays intended for use as expansion shelf enclosures.

 **NOTE:** The 300 Gigabyte (GB) drive capacity (2.7 TB) version of the DR Series system does not support the addition of expansion shelf enclosures.

There are two ways to obtain the expansion shelf enclosure license (license.xml):

- By downloading the license file from the Dell Support website (support.dell.com), in which you enter your service tag or navigate to your DR Series system type, then click **Get Drivers**.
- By using an email link from Dell where the license file resides.

Once you have located the license file for expansion shelf enclosure use WinSCP to copy it to the /store/license, which is a location known by the DR Series system software.

 **NOTE:** Each added expansion shelf enclosure must be equal to or greater than each DR Series system internal drive slot capacity (0–11). Because 1 TB drives are the smallest ones supported by the expansion shelf enclosure you add, the 600 Gigabyte (GB) DR Series systems need to use 1 TB or larger sized drives in any expansion shelf enclosure added to the base system.

Syntax


```
system --license --validate
```

Result

```
License file is valid and can be installed.
```

To add a validated license for a data storage expansion shelf (enclosure), use the following DR Series system CLI command:

```
system --license --add
License file has successfully installed.
```

 **NOTE:** The recommended process for adding an expansion shelf enclosure involves the following tasks:

- Use the **system --license [--validate] [--add]** command to validate and install the license for the expansion shelf enclosure.
- Power off (if needed) the Dell MD1200 storage array, physically connect the expansion shelf enclosure to the base DR Series system, and power on the expansion shelf enclosure.
- Use the **system --add_storage --enclosure** command (for specific information, see [system --add_storage --enclosure <service tag>](#)).

system --setname --name <node_name>

Description

Sets the hostname for a DR Series system.

Syntax

```
system --setname --name acme-60
```

Result


```
Successfully updated hostname.
Restarting syslog service ... done.
```

system --setcompression [--fast] [--best]

Description

Sets the compression type to use on the data stored by a DR Series system. The options are as follows:

- **fast** — Uses the fastest compression algorithm. This is the default.
- **best** — Compresses the data to get the greatest possible space savings.

 **NOTE:** The following example shows the default option in use. For more information, see the *Dell DR Series System Administrator Guide*.

Syntax

```
system --setcompression --fast
```


Result

Successfully updated compression level.

system --setdate [--date <date>] [--timezone <Region/Zone>]

Description


Sets the date and time zone on a DR Series system.

 **NOTE:** To set a date (month/day/hour/minute) for the DR Series system, enter values using the following format where the specifying of a four-digit year [[CC]YY] and seconds [.ss] are optional: MMDDhhmm [[CC]YY][.ss].

For example, September 29, 2011 13:20:00 can be entered in any of the following ways:

- 0929132012 and 092913202012: where 0929 represents September 29, 1320 represents 13:20 in a 24-hour time format, and 12 and 2012 both represent 2012.
- 0929132012.00 and 092913202012.00: where 0929 represents September 29, 1320 represents 13:20 in a 24-hour time format, 12 and 2012 both represent 2012, and .00 represents 13:20:00.

Syntax

 **NOTE:** Respond to the prompt to stop the NTP service by issuing a **system --setntp --disable** command.

```
system --setdate --date 092913202012 --timezone US/Pacific
```

```
Please stop NTP service before changing time.
```

```
system --setntp --disable
```

Result

```
Shutting down ntpd: [ OK ]  
Fri Jun 29 13:20:00 PDT 2012
```

```
NTP service is already disabled.  
Changed the time zone to US/Pacific  
Thu Jun 29 13:20:00 PDT 2012
```

system --setntp [--add <server name>]

Description

Adds a new NTP server for use with the DR Series system.

Syntax

```
system --setntp --add 2.centos.pool.ntp.org
```

Result

```
Stopping NTP service ... Done
Adding NTP server ... Done
Starting NTP service ... Done
NTP server 2.centos.pool.ntp.org added.
```

Enter the following DR Series system CLI command to verify that the NTP server was successfully added:

```
system --show --ntp
```

```
NTP Service is      : UP
Server 1            : 0.centos.pool.ntp.org
Server 2            : 1.centos.pool.ntp.org
Server 3            : 2.centos.pool.ntp.org
```

system --setntp [--delete <server name>]

Description

Deletes an existing NTP server.

Syntax

```
system --setntp --delete 2.centos.pool.ntp.org
```

Result

```
Stopping NTP service ... Done
Removing NTP server ... Done
Starting NTP service ... Done
NTP server 2.centos.pool.ntp.org deleted.
```

system --setntp [--enable]

Description

Enables the NTP service for your DR Series system.

Syntax

```
system --setntp --enable
```

Result

```
ntp: Synchronizing with time server: [ OK ]
Starting ntpd: [ OK ]
```

To verify whether the NTP service was enabled, use the following command:

```
system --setntp --enable
NTP service is already enabled.
```

system --setntp [--disable]

Description

Disables the NTP service for your DR Series system.

Syntax

```
system --setntp --disable
```

Result

```
Shutting down ntpd:      [ OK ]
```

system --setntp [--adjust_time]**Description**

Synchronizes a DR4000 system with the NTP server.

Syntax

```
system --setntp --adjust_time
```

Result

```
Time difference less than 2 seconds. Not adjusting with server  
0.centos.pool.ntp.org  
Time difference less than 2 seconds. Not adjusting with server  
1.centos.pool.ntp.org  
Time difference less than 2 seconds. Not adjusting with server  
2.centos.pool.ntp.org
```

system --setlogin**Description**

Updates or resets the login password for the administrator of a DR Series system.

Syntax

```
system --setlogin
```

Result

```
Please enter administrator password:  
Please enter administrator's new password:  
Please re-enter administrator's new password:  
Changed administrator's password.
```

system --telnet [--enable | --disable]**Description**


Displays the current telnet access status, or you can use the command options to enable or disable telnet access for a DR Series system.

Syntax

```
system --telnet
```

Result

```
Telnet State      : Disabled
```

 **NOTE:** In this example, the **system --telnet** command output showed the telnet access status as disabled. The following example shows the command for enabling telnet access on your DR Series system. To disable telnet access, use the **system --telnet --disable** command.

```
system --telnet --enable
Successfully enabled telnet.
```

system --datacheck [--enable <all | namespace | blockmap>]

Enables one or both Data Check scan options that can be used on a DR Series system. You can individually enable **namespace** or **blockmap** scan options, or both options using the **all** scan option (which means that both the **namespace** and **blockmap** scan types will be enabled).

Description


Enables an individual Data Check scan option type (or both scan types) when used in a DR Series system CLI command.

Syntax

```
system --datacheck --enable all
```

Result

```
Data Check configuration successful: namespace and blockmap scans currently enabled.
```

 **NOTE:** This example shows **all** Data Check scan options enabled. To enable only the **namespace** or only the **blockmap** scan, simply replace the **all** option with either of the other option types you desire in the DR Series system CLI command.

system --datacheck [--disable <all | namespace | blockmap>]

Disables one or both Data Check scan option types that can be used on a DR Series system. You can individually disable **namespace** or **blockmap** scan options, or both options using the **all** scan option (which means that both the **namespace** and **blockmap** scan types will be disabled).

Description


Disables an individual Data Check scan option type (or both scan types) when used in a DR Series system CLI command.

Syntax

```
system --datacheck --disable all
```

Result

```
Data Check configuration successful: all scans currently disabled.
```

 **NOTE:** This example shows **all** Data Check scan options being disabled. To disable only the **namespace** or the **blockmap** scan, simply replace the **all** option with either of the other option types you desire in the DR Series system CLI command.

system --datacheck [--throttle <1-100>]

Use the Data Check **--throttle** option to specify the percentage of available DR Series system resources you want to use when running Data Check scans when the other system operations (data ingest, Replication, and Cleaner processes) are idle. The range is between 1 to 100 percent (%), and the default is 50%.

Description

Enables Data Check scans to use any percentage (1–100) of available DR Series system resource that you define. In this example, 75% of the available DR Series system resources are selected.

Syntax

```
system --datacheck --throttle 75
```

Result

```
Data Check configuration successful: throttle set to 75%.
```

system --marker [--enable] [--disable]

Description

Enables or disables the marker detection status for all of the supported backup software used with a DR Series system based on the option you use with the command.


Syntax

```
system --marker
```

Result

```
Please enter either --enable or --disable to change system-level marker settings.
```

For more information about enabling or disable marker detection settings on a DR Series system, see [system --marker \[--enable\]](#) or [system --marker \[--disable\]](#).

 **NOTE:** To display the current status of the marker detection settings, use the DR Series system CLI command: **system --show --marker.**

```
system --show --marker
```

```
Marker Detection : Enabled
```

system --marker [--disable]

Description

Disables the marker detection status for all supported backup software on a DR Series system. For example, the DR Series system supports specific versions of data management application (DMA) software like NetBackup version 6.5 and 7.1, Backup Exec 2010 and 2012, and Veeam 5.7 and 6.0. For a complete list of the supported DMAs, see the *Dell DR Series System Interoperability Guide*.

Syntax

```
system --marker --disable
```

Result

```
Successfully disabled system marker.
```

system --marker [--enable]

Description

Enables the marker detection status for all supported backup software on a DR Series system. For example, the DR Series system supports specific versions of data management application (DMA) software like NetBackup version 6.5

and 7.1, Backup Exec 2010 and 2012, and Veeam 5.7 and 6.0. For a complete list of the supported DMAs, see the *Dell DR Series System Interoperability Guide*.

Syntax

```
system --marker --enable
```


Result

Successfully enabled system marker.


system --add_storage --enclosure <service tag>

Description


Adds a data storage expansion shelf (enclosure) to a DR Series system. Each expansion shelf that is added to a DR Series system requires an individual service tag and a license. For details about the maximum allowable expansion shelves and their capacities, see the *Dell DR Series System Administrator Guide* at dell.com/support/manuals.


 **NOTE:** The 300 Gigabyte (GB) drive capacity (2.7 TB) version of the DR Series system does not support the addition of expansion shelf enclosures.

For more information about the required licenses, see [system --show \[--license\] \[--verbose\]](#) and [system --license \[--validate\] \[--add\]](#).

 **NOTE:** The recommended process for adding an expansion shelf enclosure involves the following tasks:

- Use the **system --license [--validate] [--add]** command to validate and install the license for the expansion shelf enclosure. For specific information, see [system --license \[--validate\] \[--add\]](#).
- Power off (if needed) the Dell MD1200 storage array, physically connect the expansion shelf enclosure to the base DR Series system, and power on the expansion shelf enclosure.
- Use the **system --add_storage --enclosure <service tag>** command .

 **NOTE:** Each added expansion shelf enclosure must be equal to or greater than each DR Series system internal drive slot capacity (0–11). Because 1 TB drives are the smallest one supported by the expansion shelf enclosure you add, the 600 Gigabyte (GB) DR Series system needs to use 1 TB or larger sized drives in any expansion shelf enclosure added to the base system.

 **NOTE:** To verify the current types of storage on a DR Series system, use the DR Series system CLI command: **system --show --storage**. For more information, see [system --show \[--storage\]](#).

Syntax

```
system --add_storage --enclosure CTKHVW1
```

Result

```
WARNING: IO to the box will be stopped during enclosure addition.
```


```
Do you want to continue (yes/no) [n]? y  
Enclosure: "CTKHVW1" added successfully.
```

system --storage [--blink] [--type <internal | external>] [--service_tag <service tag>] [--disk <slot num>]

Description

Turns on an LED that is used in locating a specific physical disk or data storage expansion shelf (using the **system --storage** command) in the DR Series system. Select from the following DR Series system CLI command options:

- **--blink**: turns on LED on the physical disk or expansion shelf to identify it.
- **--type <internal | external>**: identifies storage as an internal physical disk or external expansion shelf.
- **--service_tag <service tag>**: identifies physical disk or expansion shelf by its unique service tag.
- **--disk <slot num>**: identifies the disk slot number (if no disk slot is defined, it globally affects all disks).

 **NOTE:** There is a counterpart to this command, in which you can turn off the LED that aids in locating the physical disk or expansion shelf. For more information, see [system --storage \[--unblink\] \[--type <internal | external>\] \[--service_tag <service tag>\] \[--disk <slot num>\]](#).

Syntax

```
system --storage --blink --type external --service_tag HCMOPT3
```

Result

Turned on blinking for all disks in enclosure "HCMOPT3".

system --storage [--unblink] [--type <internal | external>] [--service_tag <service tag>] [--disk <slot num>]

Description

Turns off an LED that is used in locating a specific physical disk or data storage expansion shelf (using the **system --storage** command) in the DR Series system. Select from the following DR Series system CLI command options:

- **--unblink**: turns off LED on the physical disk or expansion shelf.
- **--type <internal | external>**: identifies storage as an internal physical disk or external expansion shelf.
- **--service_tag <service tag>**: identifies physical disk or expansion shelf by its unique service tag.
- **--disk <slot num>**: identifies the disk slot number (if no disk slot is defined, it globally affects all disks).

Syntax

```
system --storage --unblink --type external --service_tag CTKHVW3
```

Result

Turned off blinking for all disks in enclosure "CTKHVW3".

system --mgmt_traffic

Description

The command configures Webserver or Telnet to use a specific network interface.

Syntax

```
system --mgmt_traffic [--add] [--type <Webserver|Telnet>] [--interface <bondN|ethN|lo>]
ethN|lo>] [--update] [--type <Webserver|Telnet>] [--interface <bondN|
ethN|lo>]
ethN|lo>] [--delete] [--type <Webserver|Telnet>]
```

```

--add          Add access network configuration.
--update       Update access network configuration.
--delete       Delete access network configuration.
--type         Access type <Webserver|Telnet> to configure.
--interface    Interface to use for access [bond(0-N)|eth(0-N)].

```

Result

```

Successfully added application webserver.
Restarting webserver service ... done.

```

system --backup_traffic

Description

The command specifies the network interfaces to use for backup network traffic.

Syntax

```

system --backup_traffic [--add] [--type @NFS|CIFS|OST|RDS#] [--interface
@bond(0-N)|eth(0-N)|lo#]
                                [--update] [--type @NFS|CIFS|OST|RDS#] [--interface @bond(0-N)|
eth(0-N)|lo#]
                                [--delete] [--type @NFS|CIFS|OST|RDS#]

```

```

--add          Add backup network configuration.
--update       Update backup traffic network configuration.
--delete       Delete backup traffic network configuration.
--type         Backup traffic type [NFS|CIFS|OST|RDS] to configure.
--interface    Interface to use for backup traffic.

```

Result

```

WARNING: This operation requires filesystem server restart. IO to the box will
be stopped.
Do you want to continue (yes/no) [n]? y
Successfully added application.
Restarting file system ... done.

```

system --replication_traffic

Description

The command sets the default network interface for replicating 'source' data.

Syntax

```

system --replication_traffic [--add] [--interface <bondN|ethN|lo>]
                                [--update] [--interface <bondN|ethN|lo>]
                                [--delete]

```

```

--add          Add default replication network configuration.
--update       Update default replication network configuration.
--delete       Delete default replication network configuration.
--interface    Interface to use for replicating 'source' data.

```

For example, to add the replication, run the command, `system --replication_traffic --add --interface bond0`

Result

Successfully added application replication.

system --opdup_traffic

Description

The command sets the default network interfaces for optimized copy data transfer.

Syntax

```
system --opdup_traffic [--add] [--incoming_interface <bondN|ethN|lo>] [--  
outgoing_interface <bondN|ethN|lo>]  
                        [--update] [--incoming_interface <bondN|ethN|lo>] [--  
outgoing_interface <bondN|ethN|lo>]  
                        [--delete]
```

--add	Add default optimized copy configuration.
--update	Update default optimized copy configuration.
--delete	Delete default optimized copy configuration.
--incoming_interface	Interface to use for receiving optimized copy data.
--outgoing_interface	Interface to use for sending optimized copy data.

For example, to add the default network interface for incoming traffic, run the command: `system --opdup_traffic --add --incoming_interface bond0`

Result

Successfully added application opdup_incoming.

system --help

Description

Displays the list of all system-related options that can be used as a reference when using the DR Series system CLI.

Syntax

```
system --help
```

Result

Usage:

```
system --show [--config]  
              [--hardware]  
              [--storage] [--type <boot|internal|external>] [--service_tag  
<service tag>]  
              [--license] [--verbose]  
              [--ntp]  
              [--version]  
              [--timezones [Region]]  
              [--upgradefile]  
              [--upgradehistory]  
              [--marker]  
              [--replication_traffic]  
              [--opdup_traffic]  
              [--backup_traffic]  
              [--mgmt_traffic]  
  
system --reboot
```

```

system --shutdown
system --upgrade
system --license [--add]

system --setname --name <node_name>

system --setcompression [--fast]
                        [--balanced]
                        [--best]

system --setdate [--date <date>]
                [--timezone <Region/Zone>]

system --setntp [--add <server name>]
               [--delete <server name>]
               [--enable]
               [--disable]
               [--adjust_time]

system --setlogin
system --telnet [--enable | --disable]

system --datacheck [--enable <all|namespace|blockmap>]
                  [--disable <all|namespace|blockmap>]
                  [--throttle <1-100>]

system --marker [--enable]
               [--disable]

system --add_storage --enclosure <service tag>

system --storage [--blink] [--type <internal|external>] [--service_tag
<service tag>] [--disk <slot num>]
               [--unblink] [--type <internal|external>] [--service_tag
<service tag>] [--disk <slot num>]

system --mgmt_traffic [--add] [--type <Webserver|Telnet>] [--interface
<bondN|ethN|lo>]
               [--update] [--type <Webserver|Telnet>] [--interface <bondN|
ethN|lo>]
               [--delete] [--type <Webserver|Telnet>]

system --backup_traffic [--add] [--type <NFS|CIFS|OST|RDS>] [--
interface <bond(0-N)|eth(0-N)|lo>]
               [--update] [--type <NFS|CIFS|OST|RDS>] [--interface <bond(0-N)|
eth(0-N)|lo>]
               [--delete] [--type <NFS|CIFS|OST|RDS>]

system --replication_traffic [--add] [--interface <bondN|ethN|lo>]
               [--update] [--interface <bondN|ethN|lo>]
               [--delete]

system --opdup_traffic [--add] [--incoming_interface <bondN|ethN|lo>]
[--outgoing_interface <bondN|ethN|lo>]
               [--update] [--incoming_interface <bondN|ethN|lo>] [--
outgoing_interface <bondN|ethN|lo>]
               [--delete]

system --help

system <command> <command-arguments>
<command> can be one of:
    --show                Displays command specific information.
    --reboot              Reboots the machine.

```

	<code>--shutdown</code>	Shuts down the machine.
	<code>--upgrade</code>	Upgrades the software on the machine.
	<code>--license</code>	Installs the license on the machine.
	<code>--setname</code>	Sets the name of the machine.
stored data.	<code>--setcompression</code>	Sets the compression type to use on the
machine.	<code>--setdate</code>	Sets the date and time zone for the
to update time.	<code>--setntp</code>	Uses network time protocol (NTP) source
	<code>--setlogin</code>	Updates the login password.
	<code>--telnet</code>	Enables or disables telnet access.
verification features.	<code>--datacheck</code>	Enables or disables online data
	<code>--marker</code>	Enables or disables markers.
	<code>--add_storage</code>	Adds an expansion shelf.
	<code>--storage</code>	Locates a disk or expansion shelf.
specific network interface.	<code>--mgmt_traffic</code>	Configure Webserver or Telnet to use a
backup network traffic.	<code>--backup_traffic</code>	Specify network interfaces to use for
replicating 'source' data.	<code>--replication_traffic</code>	Set default network interface for
optimized copy data transfer.	<code>--opdup_traffic</code>	Set default network interfaces for

For command-specific help, please type `system --help <command>`

eg:

`system --help show`

User


This topic introduces the DR Series system CLI commands that allow you to manage service and root accounts by having the ability to enable or disable these types of “user” accounts, and provide the capability to display the list of current active user accounts logged in to a DR Series system:

- `user --show [--users] [--logins]`
- `user --enable --user <service | root>`
- `user --disable --user <service | root>`
- `user --help`

User Command Usage

This topic introduces the `user` command usage:

- `user --show [options]`
- `user --enable --user [options]`
- `user --disable --user [options]`
- `user --help`

 **NOTE:** If you specify a command without supplying the expected value or option, you will be prompted to provide the correct value or option.

user --show [--users] [--logins]

Description

Displays the current status of the service and root user accounts (using the `user --show --users` command), and also displays the login types and login times on a DR Series system (using the `user --show --logins` command).

Syntax

```
user --show --users
```

Result

```
Service Account      : Disabled
Root Account         : Disabled
```

Other Examples

Displays the current status of login attempts on a DR Series system.

```
user --show --logins
User Name      Terminal   Login Time
root           pts/1      Oct 24 10:51 (10.15.13.4)
root           pts/2      Oct 23 20:41 (10.18.0.1)
root           pts/3      Oct 23 20:41 (10.15.0.13)
root           pts/5      Oct 24 09:35 (10.20.21.6)
administrator pts/6      Oct 24 12:32 (acme13.storage.local)
root           pts/7      Oct 24 12:24 (10.18.11.12)
```

user --enable --user <service | root>

Description


Enables the service or root user account on a DR Series system.

Syntax


```
user --enable --user root
```

Result

```
"root" user enabled.
```

 **NOTE:** To enable the service user account instead of the root user account, simply substitute the **service** option with the **--user** option, as shown in the following example:

```
user --enable --user service
```

 **NOTE:** If root user or service user is enabled, it gets disabled after a reboot. You must enable it again, if required.

user --disable --user <service | root>

Description

Disables the service or root user account on a DR Series system.

Syntax

```
user --disable --user root
```

Result

```
"root" user disabled.
```



NOTE: To disable the service user account instead of the root user account, simply substitute the **service** option with the **--user** option, as shown in the following example:

```
user --disable --user service
```

user --help

Description

Displays the list of all user-related options that can be used as a reference when using the DR Series system CLI.

Syntax

```
user --help
```

Result

Usage:

```
user --show [--users]
          [--logins]
```

```
user --enable --user <service | root>
```

```
user --disable --user <service | root>
```

```
user --help
```

```
user <command> <command-arguments>
```

<command> can be one of:

```
--show      Displays command specific information.
--enable    Enables a user account.
--disable   Disables a user account.
```

For command-specific help, please type `user --help <command>`

For example:

```
user --help show
```


Maintaining the DR Series System

This topic introduces the CLI commands that are useful for collecting diagnostics information, and managing the filesystem and performing system maintenance-related tasks. These CLI commands are grouped into two categories:

- The **Diagnostics** command and its options are used to collect DR Series system log file information. For more information, see [Diagnostics](#).
- The **Maintenance** command and its options are used to perform filesystem and system maintenance. For more information, see [Maintenance](#).

Diagnostics

The DR Series system CLI **Diagnostics** command lets you display, collect, and manage the diagnostic log file information for your system, which provides these benefits:

- Captures a snapshot of the current state of DR Series system operations.
- Assists Dell Support understand the sequence of DR Series system operations.
- Records DR Series system operations in the event that Dell Support needs to provide technical assistance.

The **Diagnostics** command works by collecting all system-related information that assists in understanding system operations when diagnosing a problem or error condition in the DR Series system.


The Diagnostics service runs during system startup, and listens for incoming requests sent to the DR Series system. There are two modes in which the diagnostics collection process is started:

- **Admin-Generated Mode:** when a DR Series system CLI or GUI request is made by the administrator (and the default reason is listed as admin-generated).
- **Auto-Generated Mode:** when a process or service failure is reported, the DR Series system starts collecting a wide variety of system-related information. After a successful completion of the auto-generated collection, the DR Series system also generates a system event.

 **NOTE:** Use the `alerts --show --events` or the `alerts --show --alerts` command to display or check the current events or alerts.

The Diagnostics service stores all log information in a primary log directory, and the DR Series system also maintains a backup copy of each log in a separate, secondary log directory. After each new diagnostics log is collected, the Diagnostics process computes the sizes of each of these two log location directories.


Whenever a log directory exceeds its maximum storage capacity, the oldest logs are deleted to free up space for the current logs that the DR Series system generates.

 **NOTE:** Diagnostics that you run from the GUI will run the largest bundle collection routine (the equivalent of running `diagnostics --collect --all` from the CLI). If you want to reduce the bundle collection time and file size for individual files and small bundle collection, see the options in the topics that follow.

Diagnostics Command Usage

This topic introduces the **diagnostics** command usage:

- **diagnostics --show**
- **diagnostics --collect [options]**
- **diagnostics --delete [options]**
- **diagnostics --copy [options]**
- **diagnostics --help**

 **NOTE:** If you specify a command without supplying the expected value or option, you will be prompted to provide the correct value or option.

diagnostics --show

Description

Displays a list of the diagnostics log files, by filename, size, status, and reason for generation. The diagnostics log files are a collection of all DR Series system-related information that describe the current state of your system.

Syntax

```
diagnostics --show
```

Result

```
Filename
Size      Timestamp
Status    Reason
-----
diags_2012-06-17_09-30-51.lzip  23.3MB      Sun Jun 17 16:33:12 2012  Completed

      [admin-generated]:

      generated by Administrator

acme_2012-06-20_11-39-43.lzip    36.9MB      Wed Jun 20 11:34:04 2012  Completed

      [auto-generated]:

      Service(s) "ofsck" failed
```

diagnostics --collect

Description

Generates a new diagnostics log file that represents the current state of a DR Series system. This command option is only available in the CLI.

The resulting bundle has subsets of log files and cores (if they exist) but does not include a DSET report. A DSET can be obtained with the entire bundle by using the **--all** option, or separately by using the **--dset** option.


If a DSET report is not required, running the **--collect** command can save 5 to 10 minutes from the log collection process. If core dumps exist on the system, file size can be affected by system memory capacity.

Syntax

```
diagnostics --collect
```

Result

```
Collecting diagnostics...done.  
Diagnostics file acme9_2011-11-17_17-15-52.lzip created.
```

 **NOTE:** To check how many diagnostic log files have been recently generated, enter the following commands at the system prompt:

```
pwd  
/home/administrator  
  
ls  
acme9_2012-07-18_09-48-26.lzip  
acme9_2012-07-18_10-34-48.lzip  
acme9_2012-07-25_14-09-15.lzip  
acme9_2012-07-30_14-35-30.lzip  
acme9_2012-07-30_15-25-59.lzip
```

diagnostics --collect [--name <name>]

Description

Defines a specific name for the diagnostics file you want to generate using the **--name** option with the DR Series system CLI **diagnostics --collect** command.

Syntax

```
diagnostics -collect --name diag_acme99_10-02-12
```

Result

```
Collecting diagnostics...done.  
Diagnostics file diag_acme99_10_02_12.lzip created.
```

diagnostics --collect [--reason <reason>]

Description

Defines a specific reason for generating a diagnostics file for the DR Series system using the **--reason** option with the DR Series system CLI **diagnostic --collect --name** command.

Syntax

```
diagnostics --collect --name acme9_09_17_12 --reason check-operations
```

Result

```
Collecting diagnostics...done.  
Diagnostics file acme9_09_17_12.lzip created.
```

diagnostics --collect [--force]

Description

Forces an immediate generation of a diagnostics file that collects your current system information using the **--force** option with the DR Series system CLI **diagnostic --collect --name** command.



NOTE: Use the DR Series system CLI **diagnostics --force** command when you want to override any existing system operations to generate a diagnostics log file immediately because it is a priority.

Syntax

```
diagnostics --collect --force
```

Results

```
Collecting diagnostics...done.  
Diagnostics file acme9_2012-09-15_13-53-57.lzip created.
```

diagnostics --collect [--dset]

Description

Collects the current system hardware diagnostics information that may be needed by Dell Support personnel using the **--dset** (Dell E-Support Tool) option with the DR Series system CLI **diagnostics --collect** command.

The DSET log lets you collect hardware, storage, and operating system information from the Dell DR Series system hardware appliance. This information is consolidated into a single System Configuration Report that can be used for troubleshooting or inventory collection of a system. As part of the troubleshooting process, you may be asked to provide a DSET log when you contact Dell Support.

The DSET log file is valuable to have when a smaller file is required and system hardware or firmware needs to be evaluated. This will generally take between 5 and 10 minutes.

Syntax

```
diagnostics --collect --dset
```

Result

```
Collecting diagnostics...  
DSET collection might take about 10 minutes. Please wait...done.  
Diagnostics file dset_2012-09-18_09-28-03.zip created.
```

diagnostics --collect [--logs]

Description

The command collects only logs and system configuration. Use the **--logs** option if a current system state is needed, but file size needs to be smaller for FTP transfer to Dell Support. The **--logs** option puts the current system configuration in the smallest file containing most of what Dell Support needs to start an investigation. File size can be reduced by eliminating core dumps, DSET reports, and archive files.

Syntax

```
diagnostics --collect --logs
```

Result

```
Collecting diagnostics...done.  
Diagnostics file created.
```

diagnostics --collect [--cores]

Description

The command collects only cores. Use this option if a basic bundle already exists and Dell Support only requires new core files. After the core files are collected, they are deleted from the DR Series system.

Syntax

```
diagnostics --collect --cores
```

Result

```
Collecting diagnostics...done.  
Diagnostics file created.
```

diagnostics --collect [--tcpdump]

Description

The command collects only TCP dump reports. TCP dumps may be generated by Dell Support if network troubleshooting is being performed. If a TCP dump is present on the system, run the **diagnostics --collect --tcpdump** command to collect the TCP dump reports without collecting an entire bundle. This reduces file size.

Syntax

```
diagnostics --collect --tcpdump
```

Result

```
Collecting diagnostics...done.  
Diagnostics file created.
```

diagnostics --collect [--process_dump]

Description

The command collects the file system server dump. This file is only needed if Dell Support requests process dumps.

Syntax

```
diagnostics --collect --process_dump
```

Result

```
Collecting diagnostics...done.  
Diagnostics file created.
```

diagnostics --collect [--all]

Description

Collects all of the current system information (including -- **dset**) that may be needed during any inventory collection or troubleshooting with the DR Series system. The resulting file can vary between 500MB and 15GB and includes the following:

- Old diagnostics bundles
- Core dumps
- Large archive files
- DSET reports
- Other smaller valuable log files

It will take more than 10 minutes to collect the bundle. If diagnostics are run from the GUI, the **diagnostics --collect --all** is the equivalent command in the CLI.

Syntax

```
diagnostics --collect --all
```

Result

```
Collecting diagnostics...done.  
Diagnostics file acme9_2012-09-13_09-39-51.lzip created.
```

diagnostics --delete [--name <name>]

Description

Deletes a specific existing diagnostics log file by name when using the **--name** option with the DR Series system CLI **diagnostics --delete** command.

Syntax

```
diagnostics --delete --name diags_2012-09-16_16-33-12.lzip
```

Result

```
Diagnostics delete: Successful
```

diagnostics --delete [--all]

Description

Deletes all of the diagnostics files on a DR Series system when using the **--all** option with the DR Series system CLI **diagnostics --delete** command.



CAUTION: Carefully consider before using the DR Series system CLI --delete --all command to delete all current diagnostics log files on a DR Series system. If you delete all diagnostics log files without first saving them to another location, all previous system status information that they contained is lost and unrecoverable.

Syntax

```
diagnostics --delete --all
```

Result

```
Diagnostics delete: Successful
```

diagnostics --copy --name <name> --host <user@host | ip:[:<path>>

Description

Copies a specific existing diagnostics log file by name, by appending the **--name** option, and sends this diagnostics log file to a remote system that you can define using the DR Series system CLI **diagnostics --name** and **--host** command (by defining a destination hostname or IP address and path).

Syntax

```
diagnostics --copy --name acme9_2012-09-12-12_09-37-53.lzip --host  
administrator@10.250.207.20:  
/var/diagnostics_logs
```

Result

```
administrator@10.250.207.20's password:  
acme9_2012-09-12-12_09-37-53.lzip 100% 297MB 49.5MB/s  
00:06 Diagnostics copy: Successful
```

diagnostics --help

Description

Displays the list of all diagnostics-related options that can be used when using the DR Series system CLI.

Syntax

```
diagnostics --help
```

Result

Usage:

```
diagnostics --show
diagnostics --collect [--name <name>]
                    [--reason <reason>]
                    [--force]
                    [--dset]
                    [--logs]
                    [--cores]
                    [--tcpdump]
                    [--process_dump]
                    [--all]

diagnostics --delete [--name <name>]
                    [--all]

diagnostics --copy --name <name>
                    --host <user<<host|ip>:<path>>

diagnostics --help
```

```
diagnostics <command> <command-arguments>
```

<command> can be one of:

```
--show      Displays all current diagnostic log files.
--collect   Collects diagnostic information/creates log file
for support.
--delete    Deletes one or all existing diagnostic log files.
--copy      Copies an existing diagnostic log file to a remote
machine.
```


For command-specific help, please type `diagnostics --help <command>`

eg:

```
diagnostics --help show
```

Maintenance


The DR Series system CLI **maintenance** commands lets you display the system maintenance repair progress, and manage the data repair and state of a DR Series system. Maintenance tasks let you perform basic repairs and maintain the data and the DR Series system.

 **NOTE:** Whenever the DR Series system enters or exits from the **Maintenance** mode state, all communication via CIFS, NFS, OST, or RDS is lost.

The set of **maintenance** commands and options should only be used when the DR Series system is in the **Maintenance** mode state. Dell recommends that you contact Dell Support before performing any of these DR Series system CLI commands.


The **--filesystem** commands perform maintenance operations on the DR Series system file system, the **--configuration** commands perform a backup and restore of the system configuration, the **--hardware** commands manage the appliance

hardware, the **--disk** commands manage the system disk drives, and the **--vdisk** commands manage the virtual disk drives.


 **NOTE:** This set of **maintenance** commands provide some functionality that is not available in the DR Series system GUI. To check the status of the DR Series system, use the DR Series system CLI **system --show** command to display the current status.

Maintenance Command Usage

This topic introduces the **maintenance** command usage:

 **NOTE:** Using some of the **maintenance** command options could result in the deletion of data. Carefully observe the warnings (for example, running the scan without running the repair). If you have questions, do not perform these DR Series system CLI command options without first contacting Dell Support.

- **maintenance --filesystem [options]**
- **maintenance --configuration [options]**
- **maintenance --hardware [options]**
- **maintenance --disk [options]**
- **maintenance --remote_access [options]**
- **maintenance --vdisk --check_consistency --type [options]**
- **maintenance --help**

 **NOTE:** If you specify a command without supplying the expected value or option, you are prompted to provide the correct value or option.

maintenance --filesystem [--scan_status]

Description

Displays the current filesystem checker status and scan progress for a DR Series system.

Syntax

```
maintenance --filesystem --scan_status
```

Result

```
Filesystem checker           : Scan in progress
Filesystem check status:
DataBlock Consistency Checker Stats
=====
Phase                        : INODE CRAWL
Inode check                  : IN PROGRESS
Inodes processed             : 3200 / 3498
Time left (approx)          : 4 secs
Cont Name      TotalInodes  Checked    Corrupted    Missing Data
Orphan         Status
-----
backup                0          0          0          COMPLETED
0                    0          0          0
container29          0          0          0          COMPLETED
0                    0          0          0
backupsys-60_replicate 71826      0          0          COMPLETED
71826                0          0          0
Data block check       : COMPLETED
Data blocks processed  : 422 / 422
Corrupted data chunks  : 0
```

```

Data chunk refcount mismatch      : 0
Recomputed bytes out              : 1383308872
Recomputed bytes in               : 6107833613
Recomputed % Savings              : 77.351890%
Time left (approx)                : 0
Data block check                  : NOT STARTED
NameSpace Consistency Checker Stats
=====
Namespace check                   : NOT STARTED

```

maintenance --filesystem [--scan_report [verbose]]

Description

Displays the current filesystem checker report, which is generated by the DR Series system CLI **--start_scan** command.

Syntax

```
maintenance --filesystem --scan_report
```

Result

```

Filesystem check report:
Report generated at : Tue Jun 27 14:09:14 2012
THERE IS NO PROBLEM.

```

maintenance --filesystem [--repair_status [verbose]]

Description

Displays the current filesystem repair progress for a DR Series system.

 **NOTE:** If there is no repair status to report, the DR Series system returns the status message shown under **Result**.

Syntax

```
maintenance --filesystem --repair_status
```

Result

```
Filesystem checker is not running.
```

maintenance --filesystem [--repair_history [verbose]]

Description

Displays the filesystem checker history for a DR Series system.

Syntax

```
maintenance --filesystem --repair_history
```

Result

```

0 : Filesystem check time : Mon Jun 11 14:37:43 2012
  Dry run finished at : Mon Jun 11 14:38:03 2012
  Release version : 32309
  Data verification : not enabled
  Result: No inconsistencies discovered
1 : Filesystem check time : Tue Jun 12 12:35:33 2012
  Dry run finished at : Tue Jun 12 12:36:21 2012
  Release version : 32309
  Data verification : not enabled
  Result: No inconsistencies discovered


```

```
2 : Filesystem check time : Fri Jun 15 10:09:14 2012
    Dry run finished at : Fri Jun 15 10:11:12 2012
    Release version : 32309
    Data verification : not enabled
    Result: No inconsistencies discovered
3 : Filesystem check time : Thu Jun 21 11:47:40 2012
    Dry run finished at : Thu Jun 21 11:49:22 2012
    Release version : 32309
    Data verification : not enabled
    Result: No inconsistencies discovered
```

maintenance --filesystem [--scan_restart [verify_data | verify_rda_metadata | verify_metadata]]

Description

Restarts file system checker to generate updated report.

 **NOTE:** Argument `verify_data` validates data with pre-built checksum. Argument `verify_rda_metadata` scans only OST and RDA containers. Argument `verify_metadata` scans only the namespace for all containers.

Syntax

```
maintenance --filesystem --scan_restart [verify_data| verify_rda_metadata |
verify_metadata]
```

Result

Successfully restarted filesystem scan.

maintenance --filesystem [--repair_now]

Description

Repairs any filesystem issues in a DR Series system based on the repair report findings.

Syntax

```
maintenance --filesystem --repair_now
```

Result

Successfully started cleaner.

maintenance --filesystem [--reclaim_space]

Description

Reclaims disk space that was formerly occupied by data in the recycle bin in a DR Series system using the Cleaner process. This command is what is commonly referred to as “manually” running the Cleaner process to reclaim disk space.

Syntax

```
maintenance --filesystem --reclaim_space
```

Result

Successfully started cleaner.

maintenance --filesystem [--stop_reclaim_space]

Description

Stops the disk space reclaim process in a DR Series system.

Syntax

```
maintenance --filesystem --stop_reclaim_space
```

Result

Successfully stopped cleaner.

maintenance --filesystem [--clear_quarantine]

Description

Clears a specialized quarantine folder that collects data files considered corrupted after attempts have been made to perform repairs by the filesystem. The **maintenance --filesystem** CLI commands should only be performed when the DR Series system is in its **Maintenance** mode. This command should not need to be run on a regular basis (it should only be run when a lengthy period of time has elapsed or you feel that the space in the quarantine folder needs to be reclaimed).

Syntax

```
maintenance --filesystem --clear_quarantine
```


Result


Successfully performed quarantine cleanup.

maintenance --filesystem [--start_scan [verify_data | verify_rda_metadata | verify_metadata]]

Description

Starts file system checker for any consistency issues.

 **NOTE:** Argument `verify_data` validates data with pre-built checksum. Argument `verify_rda_metadata` scans only OST and RDA containers. Argument `verify_metadata` scans the namespace for all containers.

 **NOTE:** Be aware that using this command places the files system into a read-only mode and pauses all active replications. When the DR Series system enters **Maintenance** mode, an alert is sent that indicates this operational change.

Syntax

```
maintenance --filesystem --start_scan [verify_data | verify_rda_metadata | verify_metadata]
```

Result

This operation will make the filesystem read-only and pause all active replications.

"verify_data" option will check for data consistency issues in the filesystem. This might take long time to complete.

```
Do you want to continue (yes/no) [n]? y
Please enter the administrator password:
```

Filesystem check started successfully.

To see the status, please execute "maintenance --filesystem--scan_status".

If you enter the **maintenance --filesystem** command when the DR Series system is not in **Maintenance** mode, the following output is displayed at the system prompt:

```
maintenance --filesystem --scan_restart
```

```
"Operation not supported as system is not in maintenance mode.  
To be able to restart scan, filesystem check must be running or waiting".
```

maintenance --filesystem [--stop_scan]

Description

Stops the filesystem scan process that verifies the data contained in a DR Series system.

Syntax

```
maintenance --filesystem --stop_scan
```

Result

This operation will stop the filesystem checker and put the system back into operational mode.

```
Do you want to continue (yes/no) [n]? y  
Please enter the administrator password:  
Filesystem check stopped successfully.
```

maintenance --configuration [--backup]

Description

Backs up the current DR Series system configuration.

Syntax

```
maintenance --configuration --backup
```

Result

```
Configuration saved successfully.
```

maintenance --configuration [--restore]

Description

Restores a previously backed up DR Series system configuration and overwrites the current configuration on the system.

Syntax

```
maintenance --configuration --restore
```

Result


```
WARNING: Restore will overwrite existing configuration from the previous backup.
```

```
Previous backup was taken at time: "Tue Sep 26 16:35:03 2012".  
All configuration changes after previous backup will be lost.  
Do you want to continue (yes/no) [n]? y  
Configuration is restored successfully.
```

maintenance --configuration [--reinit_dictionary]

Description

Reinitializes the dictionary on a DR Series system. Using the **--reinit_dictionary** command is not considered a commonly performed function. Because the dictionary acts as an index that maps each chunk of data to a specific location, it is referenced during data ingests to determine if the DR Series system has seen this data before. When you reinitialize the dictionary, all entries that indicate whether there were previously archived data locations are removed. As a result, during new data ingests the DR Series system will be unable to detect any duplicates based on the existing archived data.

 **NOTE:** Use caution when considering whether you should reinitialize the dictionary. This type operation is only performed rarely, and when performed, only under special circumstances. Contact and consult with Dell Support before you use this command.

Syntax

You will need to type `yes` to continue or `no` to return to the system prompt when you are prompted whether you want to continue with this process.

```
maintenance --configuration --reinit_dictionary
```

```
Please enter administrator password:
```

```
WARNING: ALL DICTIONARY DATA WILL BE ERASED!  
Do you want to continue (yes/no)?
```

```
stop Filesystem... Done.  
Initializing Dictionary... Done.  
Restart Filesystem... Done.
```

maintenance --hardware [--reinit_nvram]

Non-volatile RAM (NVRAM) is the type of memory that retains its contents even when power to it is turned off. This is an important component of the DR Series system that is crucial to normal data operations

Description

Initializes the NVRAM that resides on the Dell DR Series system hardware appliance on which the DR Series system software is installed.

 **CAUTION:** Carefully consider before attempting to use the DR Series system CLI **--reinit_nvram** command. This command should only be used under the direction of Dell Support because it permanently erases all data stored on the NVRAM in the Dell DR Series system hardware appliance. This command is only to be used when replacing the NVRAM in your hardware appliance. Contact Dell Support and seek assistance before you use this command.

Syntax

```
maintenance --hardware --reinit_nvram
```

Result

```
Please enter administrator password:  
WARNING: ALL NVRAM DATA WILL BE ERASED!  
Do you want to continue (yes/no)?
```

Type `yes` to continue or `no` to return to the system prompt.

maintenance --hardware [--restore_hw_db]

Description

Restores and repairs the Hardware Health Monitor database for a DR Series system.

Syntax

```
maintenance --hardware --restore_hw_db
```

Result

```
WARNING: All previous Event & Alert information will be deleted.  
Do you want to continue? (yes/no) [n]? y  
Please enter the administrator password:  
The Hardware Health Monitor has been successfully restored.
```

maintenance --hardware [--network_reconfigure]

Description

Reconfigures the network interface for a DR Series system.

Syntax

```
maintenance --hardware --network_reconfigure
```

Result

```
Shutting down interface bond0      :  
[ OK ]  
Shutting down loopback interface:           [ OK ]  
Bringing up loopback interface:           [ OK ]  
Bringing up interface bond0:  
Determining IP information for bond0... done. [ OK ]  
Network settings configured successfully.  
result: 0
```

maintenance --hardware [--motherboard_replaced]

Description

Updates the motherboard service tag on all signature partitions. The system must be in manual intervention mode for this command to execute. This command applies to systems that have an external enclosure attached.

If a motherboard is replaced in the DR Series system, the service tag should be blank from service inventory. That service tag should be reprogrammed to match the existing system service tag before the on-site technician leaves; therefore, this command should not be required. However, if the service tag is changed for some reason, this command will need to be executed to update the external drives to match the new service tag. A second scenario is when migrating an enclosure from one DR Series system to another. This command would need to be executed to match the migrated enclosures drives to the new service tag.

Syntax

```
maintenance --hardware --motherboard_replaced
```

maintenance --disk [--make_standby [slot num]] [--type <internal | external-<num> | service tag>] --clear_foreign]

Description

Creates a standby disk for a DR Series system.

Syntax

The **--make_standby [slot num]** command option changes the state of a physical disk (making disk 3 in this example the standby). The slot number (0-11) that is defined in the command identifies the physical disk to set as the hot-swap spare.


```
maintenance --disk --make_standby 3
```

The **--type <internal | external-<num> | service tag>** command option manages the standby disk type (by specifying it as internal or external, and if external which enclosure number, or by its service tag).

```
maintenance --disk --type external-1
```

The **--clear_foreign** command changes the state of a physical disk. Use this command when inserting a disk from another appliance, or the disk had been used in a different RAID configuration. After installing, you must enter the following command at the system prompt:

```
maintenance --disk --clear_foreign
```

 **NOTE:** The output of the DR Series system CLI **system --show --hardware** command lists the current states of the system disks. One possible state is *foreign*, which indicates that the **--clear_foreign** command needs to be run. In addition, an alert is generated if the DR Series system detects that any of the disks were in a foreign state.

maintenance --remote_access [--show]

Description

The command shows remote access information.

Syntax

```
maintenance --remote_access --show
```

Result

```
Remote Access Device
Device Type           : iDRAC7 Enterprise
iDRAC Ports          : Present
IPMI Version         : 2.0
System GUID          : 3157304f-c0b6-4a80-3910-00564cxxxxxxx
Number of Possible Active Sessions : 5
Number of Current Active Sessions  : 0
Enable IPMI Over LAN : Yes
SOL Enabled          : Yes
MAC Address          : 78-45-C4-EC-xx-xx

IPv4 Address
IP Address Source   : Static
IP Address          : 10.250.241.xxx
IP Subnet           : 255.255.xxx.x
IP Gateway          : 10.250.xxx.x
```

maintenance --remote access [--enable]

Description

The command enables the iDRAC access (default: DHCP).

Syntax

```
maintenance --remote access --enable
```

maintenance --remote_access [--static_ip] [--ip <IPv4/IPv6 address>] [--netmask <netmask>] [--gateway <IPv4/IPv6 address>] [--device <lom1|lom2|lom3|lom4>]

Description

The command assigns a static IP address for Integrated Dell Remote Access Controller (iDRAC).

Syntax

```
maintenance --remote_access [--static_ip] [--ip <IPv4/IPv6 address>] [--netmask <netmask>] [--gateway <IPv4/IPv6 address>] [--device <lom1|lom2|lom3|lom4>]
```

 --static_ip Assign a static IP address for Integrated Dell Remote Access Controller (iDRAC).

 --ip Static IP address to use.

 --netmask Netmask for the assigned static IP address.

 --gateway Gateway for routing.

 --device Network device for iDRAC. By default, if you do not specify a device, the iDRAC port will be used.

For example, to enable the remote access, you can run a similar command like the one below:

```
maintenance --remote_access --enable --static_ip --ip 10.250.241.167 --netmask 255.255.252.0 --gateway 10.250.240.1
```

Result

```
Successfully enabled remote access
```

maintenance --remote access [--disable]

Description

The command disables the iDRAC access (default: DHCP).

Syntax

```
maintenance --remote access --disable
```

Result

```
Successfully disabled remote access
```

maintenance --vdisk --check_consistency --type <boot|internal|external> [--service_tag <service tag>]

Description

Manages virtual disk drives.

- check_consistency — Starts vdisk consistency check.

- `type` — Type of the vdisk (boot/internal/external).
- `service_tag` — Service tag of the external storage.

Syntax

```
maintenance --vdisk --check_consistency --type internal
```

Result

Vdisk check: Successful.

maintenance --help

Description

Displays the list of maintenance-related options that can be used as a reference when using the DR Series system CLI.

Syntax

```
maintenance --help
```

Result

Usage:

```

maintenance --filesystem [--scan_status]
    [--scan_report [verbose]]
    [--repair_status [verbose]]
    [--repair_history [verbose]]
    [--scan_restart [verify_data | verify_rda_metadata |
verify_metadata]]
    [--repair_now]
    [--reclaim_space]
    [--stop_reclaim_space]
    [--clear_quarantine]
    [--start_scan [verify_data | verify_rda_metadata |
verify_metadata]]
    [--stop_scan]

maintenance --configuration [--backup]
    [--restore]
    [--reinit_dictionary]

maintenance --hardware [--reinit_nvram]
    [--restore_hw_db]
    [--network_reconfigure]
    [--motherboard_replaced]

maintenance --disk [--make_standby [slot num]] [--type <internal |
external-<num> | service tag>]
    [--clear_foreign]

maintenance --remote_access [--show]
    [--enable] [--static_ip] [--ip <IPv4/IPv6 address>] [--netmask
<netmask>] [--gateway <IPv4/IPv6 address>]
    [--device <lom1|lom2|lom3|lom4>]
    [--disable]

maintenance --vdisk --check_consistency --type <boot | internal |
external> [--service_tag <service tag>]

maintenance --help

maintenance <command> <command-arguments>
<command> can be one of:

```

```

--filesystem      Maintenance operations on filesystem.
--configuration   Backup/Restore system configuration.
--hardware        Manage appliance hardware.
--disk            Manage disk drives.
--remote_access   Manage Integrated Remote Access Controller
(iDRAC).
--vdisk           Manage virtual disk drives.
```

For command-specific help, please type `maintenance --help <command>`

eg:

```
maintenance --help filesystem
```

Managing DR Series System Storage Operations

This topic introduces the DR Series system CLI commands that you can use for configuring and managing DR Series system backup operations, replication operations, and scheduling when to run Replication and disk Cleaner operations.

The DR Series system CLI commands that provide these capabilities are grouped into the following categories:

- **Connections:** configuring/managing connections to storage containers
- **Containers:** configuring/managing storage and replication relationships
- **Replication:** configuring/managing replication operations
- **Schedule:** configuring/managing Replication and Cleaner schedules for the DR Series system

System Storage Operation Commands

This topic introduces the DR Series system CLI system storage operation commands that allow you to manage the connections to both storage and replication containers, manage these containers, and manage both storage and replication operations:

- **connection:** for more information, see [Connection Command Usage](#).
- **container :** for more information, see [Container Command Usage](#).
- **replication:** for more information, see [Replication Command Usage](#).
- **schedule:** for more information, see [Schedule Command Usage](#).


Connection

This topic introduces the set of DR Series system CLI commands that allow you to manage, configure, and display connection-related settings for containers on a DR Series system. For more information, see [Connection Command Usage](#).

Connection Command Usage

This topic introduces the **connection** command usage:

- **connection --show [options]**
- **connection --add --name --type [options]**
- **connection --update --name --type [options]**
- **connection --delete --name --type [options]**
- **connection --enable --name --type [options]**
- **connection --disable --name --type [options]**
- **connection --help**

 **NOTE:** If you specify a command without supplying the expected value or option, you are prompted to provide the correct value or option.

connection --show [--name <name>]

Description

Displays the status of a specific existing container connection that you define by name (**backup**) on a DR Series system.

Syntax

```
connection --show --name backup
```

Result

```
Container Name           : backup
NFS connection IP addresses : *
NFS connection Root map  : root
NFS connection options   : rw
NFS connection Enabled    : Yes
NFS connection status    : Available
CIFS connection IP addresses : *
CIFS connection Enabled   : Yes
CIFS connection status   : Available
```

connection --show [--name <name>] [--type <NFS|CIFS|OST|RDS>] [--verbose]

Description

Displays the status of all existing container connections on a DR Series system (this example shows containers configured for NFS, CIFS, None, OST, and RDS connections).



NOTE: In addition to displaying the current status of an existing container connection, this command also verifies if an existing container connection is disabled (by listing its status as offline).

Syntax

```
connection --show
```

Result

Container Name	Connection Type
backup	NFS, CIFS
Target	RDS
avc	RDS

Other Examples

Display the status of a specific existing OST container connection (**backup**) by defining it by name using the **--name backup** command on a DR Series system:

```
connection --show --name backup
Container Name           : backup
NFS connection IP addresses : *
NFS connection Root map  : root
NFS connection options   : rw
NFS connection Enabled    : Yes
NFS connection status    : Available
CIFS connection IP addresses : *
CIFS connection Enabled   : Yes
CIFS connection status   : Available
```

Display the detailed status of a specific container connection (**backup**) by defining it by name using the **--name backup** command and defining the specific filesystem protocol type (**--type nfs**) on a DR Series system:

```
connection --show --name backup --type nfs
Container Name           : backup
NFS connection IP addresses : *
NFS connection Root map  : root
NFS connection options   : rw
NFS connection Enabled   : Yes
NFS connection status    : Available
```

Display the complete status of all existing container connections by using the **--verbose** command on a DR Series system (this example only shows a partial display of the total output):

```
connection --show --verbose
Container Entry ID      : 1
Container Name          : backup
NFS connection Entry ID : 25
NFS connection IP addresses : *
NFS connection Root map  : root
NFS connection options   : rw
NFS connection Enabled   : Yes
NFS connection status    : Available
CIFS connection Entry ID : 26
CIFS connection IP addresses : *
CIFS connection Enabled   : Yes
CIFS connection status    : Available

Container Entry ID      : 2
Container Name          : _1234
NFS connection Entry ID : 3
NFS connection IP addresses : *
NFS connection Root map  : root
NFS connection options   : rw
NFS connection Enabled   : Yes
NFS connection status    : Available

Container Entry ID      : 3
Container Name          : 12345678
NFS connection Entry ID : 4
NFS connection IP addresses : 10.3.3.3
NFS connection Root map  : nobody
NFS connection options   : ro
NFS connection Enabled   : Yes
NFS connection status    : Available
CIFS connection Entry ID : 5
CIFS connection IP addresses : 10.2.2.2,10.3.3.3,10.3.4.4
CIFS connection Enabled   : Yes
CIFS connection status    : Available
```

connection --show [--verbose]

Description

Displays the complete status of all container connections on a DR Series system.

Syntax

```
connection --show --verbose
```

Result

```
Container Entry ID      : 1
Container Name          : backup
```

```

NFS connection Entry ID      : 25
NFS connection IP addresses  : *
NFS connection Root map     : root
NFS connection options      : rw
NFS connection Enabled       : Yes
NFS connection status       : Available
CIFS connection Entry ID    : 26
CIFS connection IP addresses : *
CIFS connection Enabled     : Yes
CIFS connection status      : Available


Container Entry ID          : 2
Container Name              : 1234
NFS connection Entry ID    : 3
NFS connection IP addresses : *
NFS connection Root map    : root
NFS connection options     : rw
NFS connection Enabled     : Yes
NFS connection status      : Available

```

connection --add --name <name> --type <NFS|CIFS|OST|RDS> [--clients <ip address>] [--rootmap <nobody|root|administrator>] [--options <nfs options>] [--capacity <positive integer>]

Description

Specifies connection type, client IP addresses, defines rootmap privileges, sets mounting options for an NFS connection, and setting a capacity for an OST or RDS connection. NFS and CIFS connection types do not recognize a set capacity that is defined using a positive integer in the **--capacity** option.

 **NOTE:** NFS mounting options include read-write (rw), read-only (ro), and insecure.

- rw—allows read-write access.
- ro—allows read-only access.
- insecure—allows replies to be made to requests before changes in request are made.

Syntax

```
connection --add --name ost2 --type ost --capacity 10
```

Result

```


Successfully added connection entry.
OST connection Quota      : 10
OST connection Enabled   : Yes

```

connection --update --name <name> --type <NFS|CIFS|OST|RDS> [--clients <ip address>] [--rootmap <nobody|root|administrator>] [--options <nfs options>] [--capacity <positive integer>]

Description

Updates or modifies the connection values on an existing container connection on a DR Series system.

 **NOTE:** The following DR Series system CLI **connection** command options (**--clients**, **--rootmap**, **--options**, and **--capacity**) apply selectively to specific container type connections.

For example:

- **--clients** command option only applies to NFS and CIFS type container connections.

- **--rootmap** and **--options** command options apply only to NFS type container connections.
- **--capacity** command option only applies to OST or RDS container connections, and lets you specify a positive integer value to represent the capacity size in Gigabytes (GB). By default, OST and RDS type container connections are unlimited.

Syntax

```
connection --update --name dataStorage3 --type nfs --clients 10.27.22.11
--options ro,rw
```

Result

```
Successfully updated connection entry.
NFS connection IP addresses      : 10.27.22.11
NFS connection Root map         : administrator
NFS connection options          : ro,rw
NFS connection Enabled          : Yes
```

connection --delete --name <name> --type <NFS|CIFS|OST|RDS> [--clients <ip address>]

Description

Deletes an existing container connection type on a DR Series system.

Syntax

```
connection --delete --name dataStorage3 --type nfs --clients 10.27.22.11
```

Result

```
Successfully deleted connection entry.
```

connection --enable --name <name> --type <NFS|CIFS|OST|RDS>

Description

Enables an existing container connection type that was disabled on a DR Series system.

Syntax

```
connection --enable --name dataStorage3 --type nfs
```

Result

```
Successfully updated connection entry.
NFS connection IP addresses      : 10.27.22.11
NFS connection Root map         : administrator
NFS connection options          : rw,ro
NFS connection Enabled          : Yes
```

connection --disable --name <name> --type <NFS|CIFS|OST|RDS>

Description

Disables an existing container connection type (NFS, CIFS, OST or RDS) on a DR Series system.

Syntax

```
connection --disable --name acme3 --type ost
```

Result

```
Successfully updated connection entry.
OST connection Quota              : Unlimited
```

OST connection Used Capacity : 5.0 GB
OST connection Enabled : No

connection --help

Description

Displays the listing of user and related options that you can use as a reference when using the DR Series system CLI.

Syntax

connection --help

Result

Usage:

```
connection --show [--name <name>]
                  [--type <NFS | CIFS | OST | RDS>]
                  [--verbose]

connection --add --name <name>
              --type <NFS | CIFS | OST | RDS>
              [--clients <ip address>]
              [--rootmap <nobody | root | administrator>]
              [--options <NFS mount export options>]
              [--capacity <Positive decimal number>]

connection --update --name <name>
              --type <NFS | CIFS | OST | RDS>
              [--clients <ip address>]
              [--rootmap <nobody | root | administrator>]
              [--options <NFS mount export options>]
              [--capacity <Positive decimal number>]

connection --delete --name <name>
              --type <NFS | CIFS | OST | RDS>
              [--clients <ip address>]

connection --enable --name <name>
              --type <NFS | CIFS | OST | RDS>

connection --disable --name <name>
              --type <NFS | CIFS | OST | RDS>

connection --help

connection <command> <command-arguments>
<command> can be one of:
    --show      Displays the current connections on a container.
    --add       Adds a new connection to a container.
    --update    Updates an existing connection.
    --delete    Deletes an existing connection.
    --enable    Enables access to a container through a connection.
    --disable   Disables access to a container through a connection.
```

For command-specific help, please type connection --help <command>

eg:
connection --help show

Container


This topic introduces the set of DR Series system CLI commands that allow you to perform the following tasks:

- Display the status of all current containers (summary or detail)
- Create (and name) new containers (the DR Series system limits support to 32 containers)
- Delete existing containers

Container Command Usage

This topic introduces the **container** command usage:

- **container --show [options]**
- **container --add --name**
- **container --delete --name [options]**
- **container --marker --name <name> [--enable options] [--disable options]**
- **container --delete_files --name <name>**
- **container --help**

 **NOTE:** If you specify a command without supplying the expected value or option, you will be prompted to provide the correct value or option.

container --show

Description

Displays a list of all current containers in a DR Series system.

Syntax

```
container --show
```

Result

```
Container Entries are:
backup
acme-59_replicate
acmeStorage1
acmeStorage2
acmeStorage3dataStorage3
```

container --show [--name <name>] [--verbose]

Displays the summary status of an existing container in a DR Series system that you specify using the **container --show --name** command.

Syntax

```
container --show --name acme-41-cifs-1
```

Result

```
Container Name           : acme-41-cifs-1
Container Path           : /containers/acme-41-cifs-1
Container Marker         : commvault
```

Other Examples

Displays the detailed status of an existing container that you specify by name using the **container --show --name --verbose** command:

```
Container Name           : acme55-S2
Container Path           : /containers/acme55-S2
Container Marker         : None
NFS connection IP addresses : *
NFS connection Root map  : root
NFS connection options   : rw
NFS connection Enabled   : Yes
NFS connection status    : Available
CIFS connection IP addresses : *
CIFS connection Enabled  : Yes
CIFS connection status   : Available
Replication Role        : Source
Replication Target System : acme-85
Replication Target System IP : 10.20.22.20
Replication Target Container : acme85-S2
Replication Enabled      : Yes
Replication Compression Enabled : Yes
Replication Encryption   : AES 128-bit
```

container --add --name <name>

Description


Creates and names a new container in a DR Series system.

Syntax

```
container --add --name acme99
```

Result

Container "acme99" created successfully.

 **NOTE:** Container names cannot exceed 32 characters in length and cannot start with a number. The /, #, and @ special characters are not allowed.

container --delete --name <name>

Description


Deletes an existing NFS or CIFS container by name from a DR Series system.

Syntax

```
container --delete --name acme49
```

Result

Error: Container has to be empty before deleting the container. Please delete all File(s) and Directories in the container.

 **NOTE:** Before you can delete a specific NFS or CIFS container, the connection to the container must be disabled before you can delete its files and directories. For details, see [connection --disable --name <name> --type <NFS|CIFS|OST|RDS>](#).


Other Examples

Deletes any existing NFS or CIFS container type and the data files within the specified container by combining the **--delete** and the **--delete_files** DR Series system CLI commands:

```
container --delete --name acme_17 --delete_files
```

WARNING: All the data in the container acme_17 will be deleted!

```
Do you want to continue? (yes/no) [n]? y
Please enter the administrator password:
Container "acme_17" marked for deletion. Please run "maintenance --filesystem --reclaim_space" to recover the storage space.
```

 **NOTE:** Be aware that it may take a fair amount of time for the DR Series system file and container deletion processes to complete and update the system status. For details on deleting the files within an OST container, see [container --delete_files --name <name>](#).

container --delete --name <name> [--delete_files]

Description

Deletes the files and the existing OpenStorage Technology (OST) container on which the files reside in a DR Series system when using the **--name** option with **--delete_files** command.

Syntax

```
container --delete --name acme4 --delete_files
```

Result

WARNING: All the data in the container acme4 will be deleted!

```
Do you want to continue? (yes/no) [n]? y
Please enter the administrator password:
Container "weasel_ost" marked for deletion. Please run "maintenance --filesystem --reclaim_space" to recover the storage space.
```

container --marker [--enable <Auto | CommVault | Networker | TSM | ARCserve | HP_DataProtector | Unix_Dump | BridgeHead>] [--disable <Auto | CommVault | Networker | TSM | ARCserve | HP_DataProtector | Unix_Dump | BridgeHead>] --name <name>

Description

Enables or disables a marker type or an automatic marker setting type (Auto) on an existing container in the DR Series system. To enable or disable the automatic marker setting type on an existing container, substitute **Auto** in place of a specific marker type (for example, **Networker** in the CLI command).

Syntax

```
container --marker --enable networker --name acme99
```

Result

Marker updated successfully.

Other Examples

Disables a Networker marker on an existing container in the DR Series system:

```
container --marker --disable networker --name acme99
Marker updated successfully.
```

container --delete_files --name <name>

Description


Deletes only the data files on an existing OpenStorage Technology (OST) container in a DR Series system (and leaves the OST container intact).

Syntax

```
container --delete_files --name acme99
```

Result

Error: Connection needs to be disabled first.

 **NOTE:** This command is only supported on OST connection type containers and the connection to the container must be disabled before you can delete its files. For details, see [connection --disable --name <name> --type <NFS|CIFS|OST|RDS>](#). To delete the files and the existing OST container on which the files resides, see [container --delete --name <name> --delete_files](#).

container --help

Description

Displays the list of container-related options that can be used as a reference when using the DR Series system CLI.

Syntax

```
container --help
```

Result

Usage:

```
container --show [--name <name>]
                [--verbose]
```

```
container --add --name <name>
```

```
container --delete --name <name>
                [--delete_files]
```

```
container --marker [--enable <Auto | CommVault | Networker | TSM | ARCserve |
HP_DataProtector | Unix_Dump | BridgeHead>]
                [--disable <Auto | CommVault | Networker | TSM | ARCserve |
HP_DataProtector | Unix_Dump | BridgeHead>]
                --name <name>
```

```
container --delete_files --name <name>
```

```
container --help
```

```
container <command> <command-arguments>
```

<command> can be one of:

```
--show          Displays the current list of containers.
--add           Adds a new container.
--delete        Deletes an existing container.
--marker        Enables/Disables marker for an existing container.
--delete_files  Deletes the files in the container.
```


For command-specific help, please type `container --help <command>`

For example:


```
    container --help show
```

Replication

This DR Series system CLI command and its options allow you to manage the status of all current replication relationships and tasks on a system by:

 **NOTE:** To allow DR Series system replication operations, you must ensure that TCP ports 9904, 9911, 9915, and 9916 are enabled. For more information about supported ports for the DR Series system, see the *Dell DR Series System Administrator Guide*.


- Displaying the current replication process status information
- Creating and defining new replication links or relationships to containers
- Deleting specific replication links
- Starting and stopping the replication process between source and target containers
- Limiting the bandwidth consumed during replication
- Resynchronizing replication between source and target containers
- Troubleshooting replication connection issues

 **NOTE:** For more information about setting a Replication schedule for daily and weekly replication operations, see [schedule --add --day <day of the week> \[--start_time <hh:mm>\] \[--stop_time <hh:mm>\] \[--cleaner\] \[--replication\]](#).

Replication Command Usage

This topic introduces the **replication** command usage:

- **replication --show [options]**
- **replication --add --name --role --peer [options]**
- **replication --update --name --role --peer [options]**
- **replication --delete --name --role [options]**
- **replication --start --name --role [options]**
- **replication --stop --name --role [options]**
- **replication --limit --speed --target [options]**
- **replication --resync --name --role [options]**
- **replication --troubleshoot --peer**
- **replication --help**

 **NOTE:** If you specify a command without supplying the expected value or option, you will be prompted to provide the correct value or option.

replication --show [--name <name>] [--role <source | target>] [--verbose] [--limits]

Description

Displays a detailed summary of replication-related information for a specific replication container in the DR Series system.

Syntax

```
replication --show --name acme-59 --role source --verbose
```


Result

```
Replication Container ID      : 16
Replication Container        : acme55-S2
```

```

Replication Entry ID      : 8
Replication Role         : Source
Replication Target MDS Port : 9915
Replication Target Data Port : 9916
Replication Target System : acme-85
Replication Target System IP : 10.20.22.20
Replication Target Container ID : 14
Replication Target Container : acme85-S2
Replication Enabled      : Yes
Replication Compression Enabled : Yes
Replication Encryption   : AES 128-bit

```

 **NOTE:** To see how to display the limits set for the replication containers, see [replication --limit --speed <<num><kbps | mbps | gbps> | default> --target <ip address | hostname>](#).

replication --show

Description

Displays the current status of all existing replication containers (and respective roles) in the DR Series system.

Syntax

```
replication --show
```

Result

Container Name	Replication Role	Status
acme-59	Source	Enabled
acmeStorage1	Source	Enabled
acmeStorage2	Source	Enabled
acmeStorage3	Target	Enabled

replication --show [--limits]

Description

Displays the limits set for your replication containers on the DR Series system.

Syntax


```
replication --show --limits
```

Result

```

Replication limits are enabled.
Host Name      Target IP      Speed Limit
acme-85        10.21.22.20   192 KBps

```


 **NOTE:** You can limit the bandwidth consumed by the replication process by setting a value in kilobytes/second (kbps), megabytes/second (mbps), gigabytes/second (gbps), or use an unlimited bandwidth (default). The minimum allowed bandwidth setting for a DR Series system is 192 kbps.

For more information, see [replication --limit --speed <<num><kbps | mbps | gbps> | default> --target <ip address | hostname>](#).

```
replication --add --name <name> --role <source | target> --peer <ip address | hostname>
[--peer_name <name>] [--replication_traffic <ip address | hostname>] [--encryption <none
| aes128 | aes256>][--username <user name>]
```

Description

Adds a new replication link to a container on the DR Series system, for which you need to define its name, role, peer ID, peer name, user name, and encryption level to apply. There are three options for encryption: none, aes128 (Advanced Encryption Standard), using 128-bit cryptographic keys, and aes256 (using 256-bit AES cryptographic keys).


 **NOTE:** Make sure that the data container you intend to replicate already exists. If it does not, the following error message displays: *Error: Container <container_name> does not exist.*

Syntax

```
replication --add --name backup --role source --peer 10.25.20.10 --encryption
aes128
```

Result

```
Enter password for administrator<10.25.20.10>:
Replication configuration updated successfully.
Replication Container           : backup
Replication Role                : Source
Replication Target System      : swsys-85
Replication Target System IP   : 10.25.20.10
Replication Target Container   : acme85-S2
Replication Enabled            : Yes
Replication Compression Enabled : Yes
Replication Encryption         : AES 128-bit
```

 **NOTE:** To verify that you have successfully added a replication link to the DR Series system (or to view the current status of existing containers), see [replication --show](#).

```
replication --update --name <name> --role <source | target> [--peer <ip address |
hostname>] [--encryption <none | aes128 | aes256>] [--username <user name>]
```


Description

Updates an existing replication link to a container in a DR Series system and allows you to change the corresponding role, peer IP address or host name, the encryption being used, and user name based on the DR Series system CLI command options you specify.

Syntax

```
replication --update --name backup --role source --peer 10.25.19.5
```


Result

 **NOTE:** If you attempt to update a container that already has replication enabled, this displays the following message:

```
Replication on backup is enabled and cannot be updated, please stop it first.
```

When replication is enabled on the container, you must first disable it before you can update it. To disable replication on a container, enter the DR Series system CLI **replication --stop** command and define the container name and role:

```
replication --stop --name <name> --role <source | target>
```

 **NOTE:** For more information about disabling replication, see [replication --stop --name <name> --role <source | target>](#).

Disables replication on a container:

```
replication --stop --name backup --role source
Replication configuration updated successfully.
Replication Container      : backup
Replication Role          : Source
Replication Target System  : acme-85
Replication Target System IP : 10.25.192.5
Replication Target Container : acme85-S2
Replication Enabled       : No
Replication Compression Enabled : Yes
Replication Encryption    : AES 128-bit
```

replication --delete --name <name> --role <source | target> [--force]

Description


Deletes an existing replication link to a container in a DR Series system.

Syntax

```
replication --delete --name acme-59-replica --role target
```

If you attempt to delete a container that already has replication enabled, this displays the following message:

```
Replication on acme-59-replica is enabled and cannot be deleted, please stop it first.
```


 **NOTE:** If the replication state of the link is enabled, you must use the **replication --stop** command to disable replication before you can delete the replication link. For more information, see [replication --stop --name <name> --role <source | target>](#).

Deletes the existing replication link to a container.

```
replication --delete --name acme-59-replica --role source
```

Result

```
Successfully deleted replication entry.
```

 **NOTE:** The DR Series system CLI **--force** command is optional, and this command allows you to force the deletion of an existing replication link (such as when communications between the source and target are not working).

replication --start --name <name> --role <source | target>

Description

Starts the replication process on an existing replication link to a container in a DR Series system.

Syntax

```
replication --start --name container2_replica --role target
```

Result

```
Replication configuration updated successfully.
Replication Container      : container2_replica
Replication Role          : Source
Replication Target System  : acme-85
Replication Target System IP : 10.20.22.20
Replication Target Container : acme85-S2
```

```
Replication Enabled           : Yes
Replication Compression Enabled : Yes
Replication Encryption        : AES 128-bit
```

replication --stop --name <name> --role <source | target>

Description

Stops the replication process on an existing replication link to a container in a DR Series system.

Syntax

```
replication --stop --name acme-59_replicate --role source
```

Result

```
Replication configuration updated successfully.
Replication Container           : acme59
Replication Role                : Source
Replication Target System       : acme-85
Replication Target System IP    : 10.20.22.20
Replication Target Container    : acme85-S2
Replication Enabled             : No
Replication Compression Enabled : Yes
Replication Encryption          : AES 128-bit
```

replication --limit --speed <<num><kbps | mbps | gbps> | default> --target <ip address | hostname>

Description

Limits the bandwidth used during replication by defining a bandwidth limit using any of the following settings:

- Kilobytes/second (kbps)
- Megabytes/second (mbps)
- Gigabytes/second (gbps)
- Unlimited bandwidth (this is the default setting); minimum allowed bandwidth setting is 192 kbps

Configures replication limits for a DR Series system.

Syntax

```
replication --limit --speed 10gbps --target acme-60
```

Result

```
Successfully updated replication limit for acme-60 to 10 Gbps.
Changing traffic control policies ... done.
```

replication --resync --name <name> --role <source | target>

Description

Resynchronizes the replication process between a source and target container in a replication relationship on a DR Series system. This command should only be used in an emergency situation with the help of Dell Support. Do not mistake this command as an ability to start a replication sync outside of the schedule window. If your intention is to start a replication outside of the window, you can either delete the schedule, or add a temporary replication window to the current schedule and delete it when the systems are in sync.

Syntax

```
replication --resync --name dataStorage3 --role source
```

Result

Successfully initiated replication resync on container dataStorage3.

replication --troubleshoot --peer <ip address | hostname>

Description

Troubleshoots the replication connections between a source and target container on a DR Series system.

Syntax

```
replication --troubleshoot --peer 10.25.19.5
```

Result

The following examples shows both successful and unsuccessful replication connection attempts:

```
Testing connection to port 9904... Connected!
Testing connection to port 9911... Connected!
Testing connection to port 9915... Connected!
Testing connection to port 9916... Connected!
Replication troubleshooting completed successfully - Connection to all ports is
OK!
```

```
replication --troubleshoot --peer acme-205
Testing connection to port 9904... Connected!
Testing connection to port 9911... Connected!
Testing connection to port 9915...
Unable to connect to socket - Connection refused
Could not connect to acme-205 on port 9915 - (Connection refused)
Testing connection to port 9916...
Unable to connect to socket - Connection refused
Could not connect to acme-205 on port 9916 - (Connection refused)
```

replication --help

Description

Displays the list of all replication-related options that can be used as a reference when using the DR4000 system CLI.

Syntax

```
replication --help
```

Result

Usage:

```
replication --show [--name <name>]
                    [--role <source | target>]
                    [--verbose]
                    [--limits]

replication --add --name <name>]
                    --role <source | target>
                    --peer <ip address | hostname>
                    [--peer_name <name>]
                    [--username <user name>]
                    [--encryption <none | aes128 | aes256>]

replication --update --name <name>
                    --role <source | target>
                    [--peer <ip address | hostname>]
                    [--encryption <none | aes128 | aes256>]
```

```

        [--username <name>]

replication --delete --name <name>
            --role <source | target>
            [--force]

replication --start --name <name>
            --role <source | target>

replication --stop --name <name>
            --role <source | target>

replication --limit --speed <<num><kbps | mbps | gbps | default>
            --target <ip address | hostname>

replication --resync --name <name>
            --role <source | target>

replication --troubleshoot --peer <ip address | hostname>

replication --help

replication <command> <command-arguments>
<command> can be one of:
    --show           Displays command specific information.
    --add            Adds a replication link to a container.
    --update         Updates a replication link to a container.
    --delete         Deletes a replication link from a container.
    --start          Starts replication.
    --stop           Stops replication.
    --limit          Limits bandwidth consumed by replication.
    --resync         Initiates a replication re-sync.
    --troubleshoot   Troubleshoots replication connection.

```

For command-specific help, please type `replication --help <command>`

For example:

```
replication --help show
```

Schedule

A schedule is the means by which you set aside specific daily or weekly time periods for performing disk space reclamation or replication operations. Disk reclamation operations recover unused disk space from DR4000 system containers in which files were deleted, and replication operations are the process by which the key data is saved only once from multiple devices to minimize excessive or redundant storage of the same data.

This set of DR Series system CLI commands allow you to perform the following tasks on a system:


- Display existing scheduled Replication and Cleaner (disk space recovery) operations
- Create new schedules for Replication and Cleaner operations
- Delete existing scheduled Replication and Cleaner operations

Schedule Command Usage

This topic introduces the **schedule** command usage:

- **schedule --show [options]**
- **schedule --add --day <Day of the week (Sunday|Monday...)> [options]**

- **schedule --delete --day <Day of the week (Sunday|Monday...)> [options]**
- **schedule --help**

 **NOTE:** If you specify a command without supplying the expected value or option, you will be prompted to provide the correct value or option.

schedule --show [--cleaner]

Description

Displays any existing Cleaner schedule for a DR Series system.

Syntax

```
schedule --show --cleaner
```

Result

```
Cleaner Schedule:
                Start  Stop
Sunday          05:00  06:00
Monday          05:00  06:00
Tuesday         05:00  06:00
Wednesday      05:00  06:00
Thursday        05:00  06:00
Friday          05:00  06:00
Saturday        05:00  06:00
```

schedule --show [--replication] [--name <name>]

Description

Displays any existing replication schedule for a DR Series system. If you do not specify a name parameter, the replication schedules for all containers are returned.

Syntax

```
schedule --show --replication --name acme55-cont1
```


Result

```
Replication Schedule:
                Start  Stop
Sunday          22:00  05:00
Monday          22:00  05:00
Tuesday         22:00  05:00
Wednesday      22:00  05:00
Thursday        22:00  05:00
Friday          22:00  05:00
Saturday        22:00  05:00
```

schedule --add --day <day of the week> [--cleaner] [--replication] [--start_time <hh:mm>] [-- stop_time <hh:mm>] [--name <name>]


Description


Creates a new Cleaner or Replication schedule for a DR Series system (or for a specific container that you define using the **--name <name>** command option) using start time and stop time setpoints.

 **NOTE:** Without any Cleaner schedule set, the DR Series system Cleaner process automatically starts within two minutes after it detects that no data ingest operation or other system operation activity is present. So, if your DR Series system runs intermittent or inconsistent ingest, readback, or replication operations, there is no need to set a Cleaner schedule (it will automatically run during periods of low or non-activity). However, if your system runs regular and consistent ingest, readback, or replication operations, you should create a Cleaner schedule that runs only during a known period of low or non-activity (for example, on a day or time period sufficient to complete this process). If your system does not meet either of these cases, you can still manually run the Cleaner. For more information, see [maintenance --filesystem \[--reclaim_space\]](#).

Syntax


```
schedule --add --day Sunday --start_time 06:00 --stop_time 22:00 --cleaner
```

 **NOTE:** Set a corresponding stop time for every start time in each Cleaner (or Replication) schedule you create. The following example shows setting up a Cleaner schedule for the remainder of the week (Monday through Saturday).

 **NOTE:** Do not select 00:00 for a start time or stop time endpoint for midnight when setting Cleaner or Replication schedules (instead, use either the 23:55 or 00:05 value).

Result


```
schedule --add --day Monday --start_time 02:00 --stop_time 22:00 --cleaner
schedule --add --day Tuesday --start_time 02:00 --stop_time 22:00 --cleaner
schedule --add --day Wednesday --start_time 02:00 --stop_time 22:00 --cleaner
schedule --add --day Thursday --start_time 02:00 --stop_time 22:00 --cleaner
schedule --add --day Friday --start_time 02:00 --stop_time 22:00 --cleaner
schedule --add --day Saturday --start_time 06:00 --stop_time 22:00 --cleaner
```

 **NOTE:** To create a Replication schedule (use the DR Series system CLI **--replication** command), and the same process shown here to schedule the start and stop times for a Replication schedule. This lets you schedule starting and stopping times for each day in the week in which you want the Replication process to run.

schedule --delete --day <day of the week> [--cleaner] [--name <name>] [--replication]

Description

Deletes a day in an existing Cleaner or Replication schedule for a DR Series system (or for a specific container that you define by name using the DR Series system CLI **--name <name>** command).

 **NOTE:** To delete days from either an existing Cleaner or Replication schedule, specify the day in the week and the schedule type.

Syntax

```
schedule --delete --day Sunday --replication
```

Result

```
Successfully updated Replication schedule.
```

schedule --help

Description

Displays the list of schedule-related options that can be used as a reference when using the DR Series system CLI.

Syntax

```
schedule --help
```

Result

Usage:

```
schedule --show [--cleaner]
           [--replication]
           [--name <name>]
```

```
schedule --add --day <Day of the week (Sunday|Monday...)>
           [--start_time <hh:mm>]
           [--stop_time <hh:mm>]
           [--cleaner]
           [--replication]
           [--name <name>]
```

```
schedule --delete --day <Day of the week (Sunday|Monday...)>
           [--cleaner]
           [--name <name>]
           [--replication]
```

```
schedule --help
```

```
schedule <command> <command-arguments>
```

<command> can be one of:

```
--show    Displays command specific information.
--add     Adds a schedule for replication/cleaner.
--delete  Deletes a replication/cleaner schedule.
```

For command-specific help, please type `schedule --help <command>`

For example:

```
schedule --help show
```

Data Integrity Checking

The DR Series system design includes an online data integrity verification feature known as Data Check, which checks for potential or unexpected data inconsistencies in the data store associated with the internal system deduplication engine. Data Check performs a series of checks for unexpected data inconsistencies as early as possible in the data ingest and backup process.


Data Check checks and verifies data both during the write process and also the data already stored on the system disks. The design purpose is to detect potential issues early enough in the data management process so that original data can be used to backup and correct any potential data inconsistencies. Data Check reports data verification issues, but it is not intended nor designed to repair these issues itself.

Any data inconsistencies that are encountered are reported as DR Series system alerts, and these filesystem errors can be repaired using the **Maintenance** mode (for more information, see [Maintenance](#)).

The Data Check feature runs continuously except for when the DR Series system enters its **Maintenance** mode (it does not run while the system is in this mode). Data Check leaves the system in an **Operational** mode when it detects an error, at which point, it sends an alert and an event.

If an alert has already been sent, but has not been cleared (for example, when repairs occur during the **Maintenance** mode), no new event is sent. Similarly, for events, one is sent for the first detected data inconsistency, and then the total number of issues detected during the scan are listed in a new event.

If Data Check is enabled, it runs in the background as a low-priority process, and changes to an idle state when the other major DR Series system operations (data ingest, replication, and cleaner) are active.

 **NOTE:** Unless otherwise noted, all later references to `datacheck` or Data Check in this guide are used interchangeably to represent the Data Check feature in the DR Series system.

About Data Check

The purpose of the Data Check feature is to perform data integrity checks to detect potential silent data inconsistencies that can affect the DR Series system disks or disk subsystems, and protect user data before there is any potential data loss.

Silent data inconsistencies can be any of the following types of disk-based data storage issues: hardware imperfections, bit rot, current spikes, disk firmware problems, and ghost writes. Data Check performs its own integral data integrity checks that detect and identify potential issues after performing the following scans:

- Priority write verify scans
- Continuous data verification scans

For more information, see [Continuous Data Verification Scans](#) and [Priority Write Verify Scans](#).

Priority Write Verify Scans

Data Check performs an early write verify scan, also known as a **namespace** scan, when files are first created or when they are modified by users. All of the modified files are flagged for priority scanning and this process is based on its timestamp—with a higher priority given to the most recently modified files. Early write verify scans are performed every five minutes when the other DR Series system operations are idle. For more information, see [About Data Check](#) and [Continuous Data Verification Scans](#).

Continuous Data Verification Scans

Data Check performs a data verification scan, also known as a **blockmap** scan, which cycles every two hours through all of the objects in the data store. Data integrity verification is done by recalculating the hash values for the underlying data, and comparing these to the stored hash values using an additional checksum process. Any unexpected data inconsistencies are reported using the DR Series system alerts process.

For more information, see [About Data Check](#) and [Priority Write Verify Scans](#).

Data Check CLI Commands

These DR Series system CLI commands allow you to perform the following Data Check-related scans and display current Data Check status. There are two sets of Data Check related DR Series system CLI commands: **system --datacheck** and **stats --datacheck**.

system --datacheck Commands

- Display the current Data Check state (enabled/disabled status for **namespace**, **blockmap**, or **all**). For more information, see [system --datacheck](#).
- Enable Data Check scans (**namespace**, **blockmap**, or **all**). For more information, see [system --datacheck \[--enable <all | namespace | blockmap>\]](#).
- Disable Data Check scans (for **namespace**, **blockmap**, or **all**). For more information, see [system --datacheck \[--disable <all | namespace | blockmap>\]](#).
- Set the percentage of available system resources to use for Data Check scans. For more information, see [system --datacheck \[--throttle <1-100>\]](#).
- Display the list of Data Check help-related options that can be used as a reference when using the CLI. For more information, see [system --help datacheck](#).

stats --datacheck Commands

- Display the variety of Data Check statistics collected by the DR4000 system. For more information, see [stats --datacheck](#).
- Reset the Data Check statistics in the DR4000 system. For more information, see [stats --reset --datacheck](#).
- Display the list of Data Check-related options that can be used as a reference when using the DR Series system CLI. For more information, see [stats --help datacheck](#).

Data Check Options

Data Check performs data integrity checks that detect potential silent data inconsistencies that can affect the system disks or disk subsystems, and protect user data. Data Check provides the following options that can be set for DR Series system data scan operations:

- Namespace (**system --datacheck --enable namespace**).
- Blockmap (**system --datacheck --enable blockmap**).
- All (**system --datacheck --enable all**); this is the default setting where both namespace and blockmap are enabled.

Data Check: Namespace Scan Option

The namespace scan option focuses on file attributes such as file size, file name, permissions, and last time modified. Data integrity verification is done using a checksum process. You can choose to enable or disable the Data Check namespace scan in the DR Series system based on the command setting you select.

Data Check: Blockmap Scan Option

The blockmap scan option identifies a specific mapping of data contained within a block, with a block being a structured form of data that the DR Series system can identify. You can choose to enable or disable the Data Check blockmap scan based on the command option you select.

Data Check: All Data Scan Option

The All scan option is one of three options that can be selected for DR Series system data scan operations. The All scan option identifies that both the namespace and blockmap options are to be included in the Data Check commands. You can choose to enable or disable Data Check scans for both namespace and blockmap in the DR Series system based on the specific command option you select.

Data Check CLI Commands

These DR Series system CLI commands allow you to perform the following Data Check-related scans and display current Data Check status. There are two sets of Data Check related DR Series system CLI commands: **system --datacheck** and **stats --datacheck**.

system --datacheck Commands

- Display the current Data Check state (enabled/disabled status for **namespace**, **blockmap**, or **all**). For more information, see [system --datacheck](#).
- Enable Data Check scans (**namespace**, **blockmap**, or **all**). For more information, see [system --datacheck \[--enable <all | namespace | blockmap>\]](#).
- Disable Data Check scans (for **namespace**, **blockmap**, or **all**). For more information, see [system --datacheck \[--disable <all | namespace | blockmap>\]](#).
- Set the percentage of available system resources to use for Data Check scans. For more information, see [system --datacheck \[--throttle <1-100>\]](#).
- Display the list of Data Check help-related options that can be used as a reference when using the CLI. For more information, see [system --help datacheck](#).

stats --datacheck Commands

- Display the variety of Data Check statistics collected by the DR4000 system. For more information, see [stats --datacheck](#).
- Reset the Data Check statistics in the DR4000 system. For more information, see [stats --reset --datacheck](#).
- Display the list of Data Check-related options that can be used as a reference when using the DR Series system CLI. For more information, see [stats --help datacheck](#).

System --Datacheck


This set of DR Series system CLI commands allow you to display the current Data Check status, enable and disable Data Check scans on the DR Series system, set the throttle percentage of system resources to use for Data Check scans, and display the system Data Check help-related options. For more information, see [System --Datacheck Command Usage](#).

System --Datacheck Command Usage

This topic introduces the **system --datacheck** command usage:

- **system --datacheck**

- **system --datacheck--enable [options]**
- **system --datacheck --disable [options]**
- **system --datacheck --throttle [options]**
- **system --help datacheck**

 **NOTE:** If you specify a command without supplying the expected value or option, you will be prompted to provide the correct value or option.

system --datacheck

Description


Displays the current status of Data Check on a DR Series system.

Syntax

```
system --datacheck
```


Result

```
Data Check : Enabled - namespace,blockmap,throttle:50%
```

 **NOTE:** This example shows that both **--namespace** and **--blockmap** scans are enabled, and the default **--throttle** setting (50%) is on for the DR Series system.

However, if both Data Check scans are disabled on a DR Series system, the following output status is displayed when the **system --datacheck** command is used:

```
system --datacheck Data Check : Disabled
```

 **NOTE:** A Data Check status of disabled indicates that both the **--namespace** and **--blockmap** scans are disabled on the DR Series system.

system --datacheck [--disable <all | namespace | blockmap>]

Disables one or both Data Check scan option types that can be used on a DR Series system. You can individually disable **namespace** or **blockmap** scan options, or both options using the **all** scan option (which means that both the **namespace** and **blockmap** scan types will be disabled).

Description


Disables an individual Data Check scan option type (or both scan types) when used in a DR Series system CLI command.

Syntax

```
system --datacheck --disable all
```

Result

```
Data Check configuration successful: all scans currently disabled.
```

 **NOTE:** This example shows **all** Data Check scan options being disabled. To disable only the **namespace** or the **blockmap** scan, simply replace the **all** option with either of the other option types you desire in the DR Series system CLI command.

system --datacheck [--enable <all | namespace | blockmap>]

Enables one or both Data Check scan options that can be used on a DR Series system. You can individually enable **namespace** or **blockmap** scan options, or both options using the **all** scan option (which means that both the **namespace** and **blockmap** scan types will be enabled).

Description


Enables an individual Data Check scan option type (or both scan types) when used in a DR Series system CLI command.

Syntax

```
system --datacheck --enable all
```

Result

Data Check configuration successful: namespace and blockmap scans currently enabled.

 **NOTE:** This example shows **all** Data Check scan options enabled. To enable only the **namespace** or only the **blockmap** scan, simply replace the **all** option with either of the other option types you desire in the DR Series system CLI command.

system --datacheck [--throttle <1-100>]

Use the Data Check **--throttle** option to specify the percentage of available DR Series system resources you want to use when running Data Check scans when the other system operations (data ingest, Replication, and Cleaner processes) are idle. The range is between 1 to 100 percent (%), and the default is 50%.

Description

Enables Data Check scans to use any percentage (1–100) of available DR Series system resource that you define. In this example, 75% of the available DR Series system resources are selected.

Syntax

```
system --datacheck --throttle 75
```

Result

Data Check configuration successful: throttle set to 75%.

system --help datacheck

Description

Displays the list of **system --datacheck** related options that can be used as a reference when using the DR Series system CLI.

Syntax

```
system --help datacheck
--datacheck - Displays statistics for online data verification.
```

Result

Usage:

```
    system --datacheck
          [--enable <all|namespace|blockmap>]
          [--disable <all|namespace|blockmap>]
          [--throttle <1-100>]

    --enable          Enables online data verification scans.
    --disable         Disables online data verification scans.
    --throttle        Sets the online data verification throttle percentage.
```


stats --datacheck

This set of DR Series system CLI commands allow you to display the current Data Check statistics gathered by the system, reset the Data Check statistics for the system, and display the statistic-based Data Check help-related options. For more information, see [Stats --Datacheck Command Usage](#).

stats --datacheck Command Usage

This topic introduces the **stats --datacheck** command usage:


- **stats --datacheck**
- **stats --reset --datacheck**
- **stats --help datacheck**

 **NOTE:** If you specify a command without supplying the expected value or option, you will be prompted to provide the correct value or option.

stats --datacheck

Description

Displays the current set of datacheck statistics on a DR Series system.

 **NOTE:** The Progress field in the statistics can indicate one of three values: **Waiting**, **Running**, and **Idle**.

- **Waiting:** Data Check is in this state because another operation is now running.
- **Running:** Data Check is in this state when running the scans.
- **Idle:** Data Check is in this state waiting for the next opportunity to run the Data Check scans.

The following example shows the status of active DR Series system operations in response to the **stats --datacheck** command on a DR Series system when Data Check is enabled.

Syntax

```
stats --datacheck
```

Result

```
Data Check                               : Enabled -
namespace,blockmap,throttle:75%
Progress                                 : Idle
Active Writes                             : No
Active System Operations                  : No
Total Detected Errors                     : 0
Last Complete Namespace Scan             : 2012-02-02 17:48:18
Last Complete Blockmap Scan              : 2012-02-02 16:33:08
Namespace Scans Completed                 : 183
Namespace Scan Entries                    : 6
Namespace Scan Errors                     : 0
Namespace Scan Start Time                 : 2012-02-02 17:43:08
Namespace Scan Progress                   : 100.00%
Blockmap Scans Completed                  : 8
Blockmap Scan Entries                     : 3
Blockmap Scan Errors                      : 0
Blockmap Scan Start Time                  : 2012-02-02 16:33:06
Blockmap Scan Progress                     : 100.00%
```

Other Examples

This example shows the output from the **stats --datacheck** command used on a DR Series system when Data Check is disabled.

```
stats --datacheck
```

```
Online Data Verification      : Disabled
Progress                      : Disabled
Active Writes                 : No
Active System Operations     : No
Total Detected Errors        : 0
Last Complete Namespace Scan  : 2012-01-24 15:50:10
Last Complete Blockmap Scan   : 2012-01-24 15:55:59
```


Additional Linux Commands

This topic introduces additional Linux commands that have limited usage when used with the DR Series system CLI:

- **grep**
- **more**

While these Linux commands are available to the user, this topic and other topics related to these commands are not intended to be a reference source for these commands. Dell recommends that you consult a Linux command reference guide for more information about these commands and how they can be used.

grep

Description

Displays the supported usage of the Linux **grep** command with the DR Series system.

Syntax

```
grep --help
```

Result

Usage: grep [OPTION]... PATTERN [FILE] ...
 Search for PATTERN in each FILE or standard input.
 Example: grep -i 'hello world' menu.h main.c

Regex selection and interpretation:

-E, --extended-regexp	PATTERN is an extended regular expression
-F, --fixed-strings	PATTERN is a set of newline-separated strings
-G, --basic-regexp	PATTERN is a basic regular expression
-P, --perl-regexp	PATTERN is a Perl regular expression
-e, --regexp=PATTERN	use PATTERN as a regular expression
-f, --file=FILE	obtain PATTERN from FILE
-i, --ignore-case	ignore case distinctions
-w, --word-regexp	force PATTERN to match only whole words
-x, --line-regexp	force PATTERN to match only whole lines
-z, --null-data	a data line ends in 0 byte, not newline

Miscellaneous:

-s, --no-messages	suppress error messages
-v, --invert-match	select non-matching lines
-V, --version	print version information and exit
--help	display this help and exit
--mmap	use memory-mapped input if possible

Output control:

-m, --max-count=NUM	stop after NUM matches
-b, --byte-offset	print the byte offset with output lines
-n, --line-number	print line number with output lines
--line-buffered	flush output on every line

```

-H, --with-filename      print the filename for each match
-h, --no-filename       suppress the prefixing filename on output
                        --label=LABEL    print LABEL as filename for standard input
-o, --only-matching     show only the part of a line matching PATTERN
-q, --quiet, --silent   suppress all normal output
                        --binary-files=TYPE assume that binary files are TYPE
                        TYPE is 'binary', 'text', or 'without-match'
-a, --text              equivalent to --binary-files=text
-I                      equivalent to --binary-files=without-match
-d, --directories=ACTION how to handle directories
                        ACTION is 'read', 'recurse', or 'skip'
-D, --devices=ACTION   how to handle devices, FIFOs and sockets
                        ACTION is 'read' or 'skip'
-R, -r, --recursive    equivalent to --directories=recurse
                        --include=PATTERN files that match PATTERN will be examined
                        --exclude=PATTERN files that match PATTERN will be skipped.
                        --exclude-from=FILE files that match PATTERN in FILE will be skipped.
-L, --files-without-match only print FILE names containing no match
-l, --files-with-matches only print FILE names containing matches
-c, --count            only print a count of matching lines per FILE
-Z, --null             print 0 byte after FILE name

Context control:
-B, --before-context=NUM print NUM lines of leading context
-A, --after-context=NUM  print NUM lines of trailing context
-C, --context=NUM       print NUM lines of output context
-NUM                    same as --context=NUM
                        --color[=WHEN],
                        --colour[=WHEN] use markers to distinguish the matching string
                        WHEN may be `always', `never' or `auto'.
-U, --binary            do not strip CR characters at EOL (MSDOS)
-u, --unix-byte-offsets report offsets as if CRs were not there (MSDOS)

```

`egrep' means `grep -E'. `fgrep' means `grep -F'.
 With no FILE, or when FILE is -, read standard input. If less than two FILES given, assume -h. Exit status is 0 if match, 1 if no match, and 2 if trouble.

Report bugs to <bug-grep@gnu.org>.

more

Description

Displays the supported usage of the Linux **more** command with the DR Series system.

Syntax

```
more --help
```

Results

```
usage: more [-dflpcsu] [+linenum | +/pattern] name1 name2 ..
```