EMC® VNXe® Series

Version 3.1

Unisphere® Command Line Interface User Guide

P/N 302-000-194 REV. 04

EMC²®

CONTENTS

CHAPTER 1

Introduction

This chapter addresses the following topics:

Overview

Unisphere CLI enables you to run commands on a system through a prompt from a Microsoft Windows or UNIX/Linux host. Use Unisphere® for managing a system. Unisphere CLI is intended for advanced users who want to use commands in scripts for automating routine tasks.

Use Unisphere CLI to manage a system. Tasks include:

- Configuring and monitoring the system.
- Managing users.
- Provisioning storage.
- Protecting data.
- Controlling host access to storage.

Storage types

Unisphere CLI supports provisioning and management of network block and file-based storage, including:

- File system storage, which contains one or more shares. Allows clients to store data and easily access file systems and shares that integrate seamlessly into:
    - Windows environments that use the CIFS protocol for file sharing, Microsoft Active Directory for authentication, and Windows directory access for folder permissions.
    - Linux/UNIX environments that use the NFS protocol for file sharing and POSIX access control lists for folder permissions.
- LUN storage, over Fibre Channel (FC) or iSCSI protocol. You can have an individual LUN or a LUN group which can contains one or more LUNs. Provides block-level storage to hosts and applications that use the FC or iSCSI protocol to access storage in the form of LUNs.
- Storage for VMware virtual machines through datastores that are accessible through either the NFS (over NFS protocol) or VMFS (over FC or iSCSI protocol) formats.

Use Unisphere CLI in scripts

Use scripts with Unisphere CLI to automate routine tasks, such as provisioning storage or scheduling snapshots to protect stored data. For example, create a script to create a snapshot of an iSCSI LUN and delete the older snapshots created before it. Customer Support does not provide sample scripts or support for custom scripting.

Set up the Unisphere CLI client

You can install and launch the Unisphere CLI client on a Microsoft Windows or UNIX/Linux computer. Unisphere CLI sends commands to the system through the secure HTTPS protocol.

Install the Unisphere CLI client

To install the Unisphere CLI client:

Procedure

1. Go to your support website.

2. Download the Unisphere CLI client for your operating system.

3. Perform the following based on your operating system:

   - On Windows, double-click the installer executable and follow the prompts. The
     default installation location is: `C:\Program Files\EMC\Unisphere CLI`

     Note

     The installation directory is added to the PATH system variable.

   - On UNIX/Linux, type: **`rpm -ihv <filename>`**,
     where `filename` is the name of the installer executable. The default installation
     location is:`/opt/emc/uemcli-<version>/bin/`,

     where `version` is the version of the client installed.

Launch the Unisphere CLI client

After installing the Unisphere CLI client, you can launch the client on a Microsoft Windows
or UNIX/Linux computer.

To launch the Unisphere CLI client, perform the following in a command prompt based on
your operating system:

Procedure

1. If you have a Windows operating system, type:

   `uemcli.exe`

2. If you have a UNIX/Linux operating system, type:

   `/usr/bin/uemcli`

Certificate verification

In order to establish a secure connection between UEM CLI and its backend server, a
Public Key infrastructure (PKI) is used. An important component of PKI, is certificate
verification. Certificate verification provides a way for a user to verify the backend server
being contacted.

When UEM CLI connects to a server requesting a secure connection, the server sends its
identification in the form of a digital certificate. The certificate usually contains the
following:

- Server name

- Trusted certificate authority (CA)

- Server's public encryption key.

The UEM CLI client may contact the server that issued the certificate (the trusted CA) and
confirm the validity of the certificate before proceeding. When the certificate is verified,
UEM CLI and its backend server will establish the connection and begin to exchange data.

Certificate verification level

The `setlevel.sh` script is used to set the certificate verification level to low or medium
after the RPM package has been installed:

`low`

    The certificate verification process will not be used to access the array.

medium

> The certificate verification process will be used to access the array.

> ---
> **Note**
>
> The default is medium.
> ---

Run the following command:

/opt/emc/uemcli-VERSION/bin/setlevel.sh (low|medium|l|m)
Then follow the prompts. The tool will guide you through the steps to set the security level.

For more information, see the section Manage SSL certificates on page 352.

Unisphere CLI syntax

Following is the syntax of an example command line:

**uemcli [*<switches>*] *<object path>* [*<object qualifier>*] *<action>*
[*<action qualifiers>*]**

Executable

All command lines begin with the executable uemcli. If you do not start each command line with uemcli, the command fails and you must rerun the command. If you run only uemcli, without any switches or commands, the list of switches and their descriptions appears.

Switches

Use local switches to configure Unisphere CLI and connect to a system. Type switches immediately after uemcli. When typing more than one switch on the same line, separate each switch with a space. All switches start with a hyphen (-).

Use Switches on page 345 provides details on all available switches.

Objects

Objects identify the type of object on which to perform an action, such as a user, host, LDAP setting, or the system you are managing. All objects are categorized into types and are nested, as parent/child, to form a path to the actual object on which to perform an action, similar to locating a file in a file system. An object type can be a parent or a child of a parent. Not all parent object types contain child objects. For example, the deduplication object type does not contain child objects.

All actions require the fully qualified path to the object. The one exception is the -help switch, which applies to an object at any level in a path. Get help on page 19 explains how to use the -help switch.

The actual object on which you perform an action is identified by an ID called an object qualifier, as explained in Object qualifiers on page 15.

Example 1
In the following example for creating a user account, the two object types are user and account:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account create
-name user1 -type local -passwd Password789! -role operator
```

Example 2
In the following example for viewing all user accounts on the system, the object types are
user and account. An object ID is not specified, so the show action is performed on
account, which displays a list of all user accounts:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account show
```

Object qualifiers

Object qualifiers are unique identifiers for objects on the system. The format is:

-<identifier> <value>

where:

- identifier — Type of object qualifier. The most common is -id.

- value — Actual object qualifier.

When you create an object, such as a user or network interface, it receives an ID, which is
the object qualifier for that object. When performing actions such as viewing, changing,
or deleting an object, you specify its object qualifier. The most common identifier is the -
id parameter. The uniqueness of the qualifier is only guaranteed in the scope of the
specified object type. All object qualifiers start with a hyphen (-).

Example
In the following example for changing the password of a user account, the object qualifier
is local_user:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account -id
local_user set -passwd NewPassword456! -oldpasswd password123
```

Actions

Actions are the operations performed on an object or object type, including creating,
changing, viewing, and deleting. Actions are always required.
provides details on each of the action commands.

Example
In the following example for changing the password of a user account, the action is set:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account -id
local_user set -passwd NewPassword456! -oldpasswd password123
```

Action qualifiers

Action qualifiers are parameters specific to actions, such as attributes or settings to
modify when changing an object. All action qualifiers start with a hyphen (-).

Example
In the following example for changing a role and password for a user account, the action
qualifiers are -passwd, -oldpasswd, and -role:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account -id
local_user set -passwd newpassword -oldpasswd password123 -role
administrator
```

Size qualifiers

Use size qualifiers to indicate a specific capacity-size value. To specify a fraction, use a period. For example, type 2.4T for 2.4 terabytes. The output for a size value displays the exact number of bytes and the specified size value:

```
Size = 1209462790557 (1.1TB)
```

The following table lists the size qualifiers. The qualifiers are case-sensitive.

Table 1 Size qualifiers

Qualifier	Measurement
K	Kilobyte
M	Megabyte
G	Gigabyte
T	Terabyte
P	Petabyte

Speed qualifiers

The following qualifiers are defined for the speed values.

The following table lists the speed qualifiers. The qualifiers are case-insensitive.

Table 2 Speed qualifiers

Qualifier	Measurement
Kbps, Kb/s	1,000 bits per second
Mbps, Mb/s	1,000,000 bits per second
Gbps, Gb/s	1,000,000,000 bits per second
KBps, KB/s	1,000 bytes per second
MBps, MB/s	1,000,000 bytes per second
GBps, GB/s	1,000,000,000 bytes per second

Action commands

When using Unisphere CLI, there are four primary action commands that you can perform on object types or objects, including creating, changing, viewing, and deleting. This section explains each of these four action commands. Unisphere CLI syntax on page 14 explains the relationship between action commands, object types, and objects.

The create action command

The create action command creates an object on the system based on the specified path to the object. If the command is successful, the new object receives an object qualifier, or ID, that identifies the object on the system.

Format

`<object> create [<action qualifiers>]`

Example

The following example uses the `create` action command to create a local user account. The new user account receives the ID local_user:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account create`
`-name local_user -type local -passwd Password789! -role operator`

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = local_user
Operation completed successfully.
```

The set action command

The `set` action command modifies, or changes, an object type or object based on the specified path and object qualifier. If the object identified by the object qualifier does not exist, an error message appears.

Format

`<object path> set <object qualifier> [<action qualifiers>]`

Example

The following example uses the `set` action command to change the password for a user account. The path `/user/account` specifies that the object type is a user account. The `-id` object qualifier identifies local_user as the user account to change:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account -id`
`local_user set -passwd NewPassword456! -oldpasswd OldPassword456!`

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = local_user
Operation completed successfully.
```

The show action command

The `show` action command displays a list of objects that exist on the system and the attributes of those objects. You can specify an object qualifier to view the attributes for a single object. The `show` action command provides qualifiers for changing the display of the output, including the format and the attributes to include. The available output formats are name-value pair (NVP), table, and comma-separated values (CSV).

Format

`uemcli [<switches>] <object> [<object qualifier>] show [{-detail | -brief | -filter <value>] [-output {nvp | table [-wrap] | csv}]`

Action qualifier

Qualifier	Description
`-output|-o`	Specify the output format. Value is one of the following:

Qualifier	Description
	• `nvp` — The name-value pair (NVP) format displays output as `name=value`. Name-value pair format on page 18 provides an example of the NVP format. • `table` — The table format displays output as a table, with column headers and rows. By default, values that are too long to fit in a column are cut off. Add `-wrap` after the table qualifier, separated by a space, so that the values wrap. Table format on page 18 provides an example of the table format. • `csv` — The comma-separated values (CSV) format is similar to the table format, but the names and values are separated by commas. Comma-separated values format on page 18 provides an example of the CSV format.
`-detail`	Display all attributes.
`-brief`	Display only the basic attributes (default).
`-filter`	Comma-separated list of attributes which are included into the command output.

Name-value pair format

```
1:      ID                  = la0_SPA
        SP                  = SPA
        Ports               = eth0_SPA,eth1_SPA
        Health state        = OK (5)

2:      ID                  = la0_SPB
        SP                  = SPB
        Ports               = eth0_SPB,eth1_SPB
        Health state        = OK (5)
```

Table format

```
ID      | SP  | Ports             | Health state
--------+-----+-------------------+--------------
la0_SPA | SPA | eth0_SPA,eth1_SPA | OK (5)
la0_SPB | SPB | eth0_SPB,eth1_SPB | OK (5)
```

Comma-separated values format

```
ID,SP,Ports,Health state
la0_SPA,SPA,"eth0_SPA,eth1_SPA",OK (5)
la0_SPB,SPB,"eth0_SPB,eth1_SPB",OK (5)
```

Example

The following command modifies the set of attributes in the show action output. For example, if you add `-filter` "ID,ID,ID,ID" to the command, in the output you will see four lines with the "ID" attribute for each listed instance:

```
1:  ID = la_0
    ID = la_0
    ID = la_0
    ID = la_0
```

uemcli /net/nas/server show -filter "ID, SP, Health state, ID, Name"

Filter format

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID           = nas_1
        SP           = SPA
        Health state = OK (5)
        ID           = nas_1
        Name         = Mynas1

2:      ID           = nas_2
        SP           = SPA
        Health state = OK (5)
        ID           = nas_2
        Name         = Mynas2
```

The delete action command

The `delete` action command removes an object from the system based on the specified object and object qualifier.

Format
<object path> <object qualifier> delete

Example
The following command deletes user account local_user1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account –id local_user1 delete

Get help

For help with using the CLI, use the `–help`, `–h`, or `–?` switch for information about the syntax, an object type, or a specific object or action command.

Help on the Unisphere CLI client

For help on the client, including the use cases, switches, and system requests, type only uemcli or include the `–help|–?` switch. provides details on all available switches.

Example
The following command displays information about the syntax and switches:

uemcli -?

```
[Get help on client options]
uemcli –help
    {CMDHELP|CMD|-upload|-download|-version|-saveUser|-removeUser|-
removeAllUsers|-default|-certList|-certClear|-certDel|-certImport}

[Get help on objects or actions]
uemcli [-d <address>] [-port <number>] [-u <user_name>] [-p
<password>] [-sslPolicy {interactive|reject|accept|store}] [-t
<seconds>] [-silent] [-noHeader] [-cmdTime] <object> [<action>] –help

[Perform an action on an object on the destination system]
uemcli [-d <address>] [-port <number>] [-u <user_name>] [-p
<password>] [-sslPolicy {interactive|reject|accept|store}] [-s
```

```
<name>[:<version>]] [-gmtoff [-|+]<HH>[:<MM>]] [-t <seconds>] [-
silent] [-noHeader] [-cmdTime] <object> [<qualifiers>] <action>
[<qualifiers>]

[Upload a file to the destination system]
uemcli [-d <address>] [-port <number>] [-u <user_name>] [-p
<password>]
    [-sslPolicy {interactive|reject|accept|store}] [-t <seconds>] [-
silent] [-noHeader] -upload -f <file_path> <type> [-<parameter>
<value> ...] [<action>]

[Download a file from the destination system]
uemcli [-d <address>] [-port <number>] [-u <user_name>] [-p
<password>] [-sslPolicy {interactive|reject|accept|store}] [-t
<seconds>] [-silent] [ noHeader] -download {-d <directory>|-f
<file_path>} <type> [-<parameter> <value> ...] [<action>]

[Display the version of this client]
uemcli -version

[Save access credentials for the destination system locally]
uemcli [-d <address>] [-port <number>] -u <user_name> -p <password> [-
silent]  -saveUser

[Remove access credentials for the destination system from this
client]
uemcli [-d <address>] [-port <number>] [-silent] -removeUser

[Remove all stored access credentials from this client]
uemcli [-silent] -removeAllUsers

[Save the destination address as the default for this client]
uemcli -d <address> -port <number> [-silent] -default
[List certificates saved for this client]
uemcli [-silent] -certList

[Delete a certificate from this client]
uemcli [-silent] -certDel <certificate_id>

[Delete all certificates from this client]
uemcli [-silent] -certClear

[Import an SSL certificate from a file]
uemcli [-silent] -certImport <file>
```

Help on parent object types

For help on parent objects types, which typically contain child object types, type the
object type followed by the -help switch to view the object types it contains.

Example
The following command displays a list of DNS object types: /net /dns is the parent
object type and [config] and [domain] are the child object types. In the output, the
items in brackets are the objects on which you perform actions, such as creating and
changing.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/dns -help

```
+- /net/dns/
         +- [config]
         +- [domain]
```

To get help on all object types, type only a forward slash (/). For example, `/ -help`.

Help on child object types

For help on child object types, which are children of parent object types, type the object type followed by the `-help` switch to view a list of supported action commands.

Example

The following command displays the action commands to set (change) and show a DNS server setting: `/net /dns` is the parent object type and `[config]` is the child object type. In the output, the items in brackets are the actions, such as creating and changing, you can perform on the specified object types:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/dns/config -?

```
Configure system DNS client settings.
Actions:
 [Set]
 /net/dns/config set -nameServer <value>

 [Show]
 /net/dns/config show [-output {nvp|csv|table[-wrap]}] [{-brief|-
detail}]
```

Help on actions

For help on an action command, type the fully qualified object parameter and action command, followed by the `-help` action qualifier.

Example

The following command displays the list of interface attributes that you can change:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/if set -?

```
Storage system address: 127.0.0.1
Storage system port: 443
HTTPS connection

/net/if -id <value> set [ -vlanId <value> ] [ -addr <value> ] [ -
netmask <value> ] [ -gateway <value> ]
Modify an existing interface.

Where:
-id <value>
Specify the ID of an interface (eg. if_0, if_3)

[Optional] -vlanId <value>
Specify the virtual LAN (VLAN) ID for the interface. The interface
uses the ID to accept packets that have VLAN tags. The value range is
1 to 4095. If the value is empty string, VLAN tagging will be
disabled.
[Optional] -addr <value>
Specify the IP address for the interface.

[Optional] -netmask <value>
Specify the subnet mask for the IPv6 interface.

[Optional] -gateway <value>
Specify the gateway for the interface.
```

Introduction

CHAPTER 2

Manage the System

This chapter addresses the following topics:

Configure general system settings

Configure general settings on the system, including:

- Enable or disable automatic failback for SP.
- Manually fail back NAS servers.
- Perform a check of the overall system health.
- Change the system name.

Note

Failover occurs when there is a hardware or software problem with an SP. This failover causes all NAS servers that run on it to fail over to the another SP with minimal disruption to connected hosts. Once the SP is fixed, and automatic failback is enabled, all NAS servers automatically fail back to their original SP.

The following table lists the general system attributes:

Table 3 General system attributes

Attributes	Description
System name	Name of the system.
Model	System model.
Platform type	Hardware platform of the system.
System UUID (virtual deployments only)	System Universally Unique Identifier (UUID) for a virtual system.
License activation key (virtual deployments only)	A key that certifies that the system is licensed and the software was obtained legally.
Product serial number	System serial number.
Auto failback (physical deployments only)	Indication of whether auto failback is enabled for the SP. Value is on or off.
Health state	Health state of the system. The health state code appears in parentheses. Value is one of the following: - Unknown (0) — Status is unknown. - OK (5) — Working correctly. - OK BUT (7) — Working correctly, but there could be a problem. - Degraded/Warning (10) — Working and performing all functions, but the performance may not be optimum. - Minor failure (15) — Working and performing all functions but overall performance is degraded. This condition has a minor impact on the system and should be remedied at some point, but does not have to be fixed immediately.

Table 3 General system attributes (continued)

Attributes	Description
	• `Major failure (20)` — Failing and some or all functions may be degraded or not working. This condition has a significant impact on the system and should be remedied immediately. • `Critical failure (25)` — Failed and recovery may not be possible. This condition has resulted in data loss and should be remedied immediately. • `Non-recoverable error (30)` — Completely failed and cannot be recovered.
`Health details`	Additional health information. See Appendix A, Reference, for health information details.

View system settings

View the current system settings.

Note

explains how to change the output format.

Format
```
/sys/general show
```

Example 1 (physical deployments only)
The following command displays the general settings for a physical system:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/general show -detail`

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection


1:    System name            = demo
      Model                  = VNXe3200
      Platform type          = EMC Storage System
      Product serial number  = demo
      Auto failback          = on
      Health state           = OK (5)
      Health details         = "The system is operating normally."
      Power (Present)        = 572 watts
      Power (Rolling Average) = 573 watts
```

Example 2 (virtual deployments only)
The following command displays the general settings for a virtual system:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/general show`

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1:      System name         = Demo
        Model               = vVNX
        Platform type       = EMC Storage System
        System UUID         = 421D3F1B-6D79-52A1-9AC7-67AE794E520E
        License activation key = CQPZQ0DJJQHR0X
        Product serial number  = VIRT14349BPJEP
        Health state        = OK (5)
```

Change general system settings

Change the name of the system, or whether automatic failback is enabled or disabled.

Format

```
/sys/general set [-name <value>] [-autoFailback {on|off}]
```

Action qualifiers

Qualifier	Description
-name	Type a name for the system.
-autoFailback (physical deployments only)	Enable or disable automatic failback. Valid values are: • On • Off

Example

The following command disables automatic failback:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/general set –autoFailback off

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manually fail back NAS servers (physical deployments only)

Manually fail back all failed over NAS servers to their original SP. If auto failback is enabled, failback occurs automatically. provides the commands for enabling automatic failback.

Format

```
/sys/general failback
```

Example

The following command fails back all NAS servers that have failed over:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/general failback

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Perform a system health check

Perform a health check of the entire system. A health check is a series of checks on the state of your system to ensure that no underlying problems exist.

Note

Before upgrading the system software, a system health check must be performed. All system components must be healthy prior to upgrading the system software. If any of the system components are degraded, the software update will fail.

Format
```
/sys/general healthcheck
```

Example
The following command performs a health check of the system:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/general healthcheck

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      Error code = tform::check_for_mirror_rebuild_3

2:      Error code = flr::check_for_transitions_3

Operation failed. Error code: 0x6000cbc
One or more of the health checks failed. Please refer to Knowledge
Base for information on how to resolve these error(s). (Error Code:
0x6000cbc)
```

Configure system information

Configure system information about the system's location and user.

The following table lists the system information attributes:

Table 4 System information attributes

Attribute	Description
Location name	Location name
Rack location	Rack location name
Contact name	Contact name for the system
Address 1	Contact address for the system
Address 2	Apartment, unit or suite number
City	City name
State	State or province name
Country	Two-letter country code
Postal Code	Postal code

Table 4 System information attributes (continued)

Attribute	Description
Contact email address	Contact email address for the system
Contact phone number	Contact phone number for the system
Comment	Notes about the system

View system information

View current system information.

Note

explains how to change the output format.

Format
```
/sys/info show
```

Example
The following command displays the general setting information for the system:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/info show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection


1: Location name          = Headquarters
   Rack location          = Lab 4
   Contact name           = Joe
   Contact email address  = joe@somemail.com
   Contact phone number   = 123456789
```

Change system information

Change the system information attributes.

Format
```
/sys/info set [-location <value>] [-rackLocation <value>] [-
contactName <value>] [-contactEmail <value>] [-contactPhone
<value>] [-addr1 <value>] [-addr2 <value>] [-city <value>] [-
state <value>] [-country <value>] [ -postalCode <value>] [-
comment <value>]
```

Action qualifiers

Qualifier	Description
-location	Specify a location name.
-rackLocation	Specify a rack location name.
-contactName	Specify the contact name for the system. This is required for new certificate creation.
-contactEmail	Specify the contact email address for the system.

Qualifier	Description
-contactPhone	Specify the contact phone number for the system.
-addr1	Specify the contact address for the system.
-addr2	Specify the apartment, unit, or suite number.
-city	Specify the city name.
-state	Specify the state.
-country	Specify the country, using a two-letter country code.
-postalCode	Specify the postal code.
-comment	Specify the text of the comment.

Example

The following command changes the system information attributes:

```
uemcli /sys/info set –location Headquarters –rackLocation "Lab 4" –
contactName Joe –contactEmail joe@somemail.com –contactPhone 123456789
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
Operation completed successfully.
```

Manage security settings

Manage system security settings.

The following table lists the system information attributes:

Table 5 Security settings attributes

Attributes	Description
FIPS 140 mode	Indicates whether the system is working in FIPS mode. Valid values are: • enabled • disabled **Note** Values are case-sensitive.

View security settings

Displays current system security settings.

Format

```
/sys/security show
```

Example

The following command displays the security settings for the system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/security show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: FIPS 140 mode   = enabled
```

Change security settings

Change the system security settings.

Format
```
/sys/security set -fips140Enabled {yes | no}
```

Action qualifiers

Qualifier	Description
-fips140Enabled	Enables or disables FIPS 140 compliance mode. Valid values are: • yes • no **Note** Values are case-sensitive.

Example
The following command changes the system security settings:

```
uemcli /sys/security set -fips140Enabled yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
Management software will be restarted. Do you want to continue?
yes / no: yes

Operation completed successfully.
```

Manage system time

The following table lists the system time attributes:

Table 6 System time attributes

Attributes	Description
Time	System time - not including the command processing delay. The difference between the requested time and the resulting time can be up to one minute due to the command processing delay. **Note** System time is affected by -gmtoff.

View system time

Display current system time.

Format
```
/sys/time show
```

Example
The following command displays the system time:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/time show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection


1: Time      = 2011-01-01 03:00:00
```

Change system time

Change the system time.

Format
```
/sys/time set {-clientTime | -utc <value>} [-force {noReboot |
allowReboot | allowDU}]
```

Action qualifiers

Qualifier	Description
-clientTime	Indicates that the system time should be synchronized with the time on the system from which the CLI is being run.
	Note
	The difference between the client time and the resulting system time can be up to one minute as a result of the command processing delay.
-utc	Specify time to set on the system (in UTC format). Format: ‹YYYY›-‹MM›-‹DD›‹hh›:‹mm›:‹ss›
	Note
	The difference between the requested time and the resulting time can be up to one minute due to the command processing delay.
-force	Specify whether to accept or decline the system reboot, which may be needed to complete the time change. If the qualifier is not specified, you will be asked to confirm the reboot if it's needed. Specify one of the following (values are case-insensitive): • noReboot • allowReboot • allowDU

Qualifier	Description
	Note `allowDU` is used if the system is in a degraded state or has one SP (data will be unavailable during its reboot). Otherwise `allowReboot` is used. In silent mode, system will be rebooted if needed.

Example

The following command accepts the system reboot:

`uemcli /sys/time set -utc "2011-05-17 14:26:20" -force allowReboot`

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully
```

Manage support configuration

Manage support configuration settings on the system, including:

- Name of IP address of proxy server.

- Port number of the proxy server.

- Name of the account on the proxy server.

- Password of the account.

The following table lists the support configuration attributes:

Table 7 Support configuration attributes

Attributes	Description
`Support proxy server address`	Name or IP address of the support services proxy server.
`Support proxy server port`	Port number of the support services proxy server
`Support proxy server user name`	Name of the account on the support proxy server.
`Support proxy server password`	Password of the account on the support proxy server.
`Automatic support contracts update enabled`	Indicates whether the system automatically updates its service contracts list once a week.

View support configuration

View the current support configuration information.

Format

`/sys/support/config show`

Example

The following command displays the support configuration:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/config
show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: Support proxy server address = 10.0.0.1
   Support proxy server port    = 8080
```

Change support configuration

Change support configuration attributes.

Format
```
/sys/support/config set { [ -supportProxyAddr <value> ] [ -
supportProxyPort <value> ] [ -supportProxyUser <value> { -
supportProxyPasswd <value> | -supportProxyPasswdSecure } ] [ -
supportProxyProtocol { http | socks } ] | -noSupportProxy } [ -
autoUpdateContracts { yes | no } ]
```

Action qualifiers

Qualifier	Description
-supportProxyAddr	Specify the name or IP address of the support services proxy server.
-supportProxyPort	Specify the port of the support services proxy server.
-supportProxyUser	Specify the user name of an account on the support services proxy server.
-supportProxyPasswd	Specify the password for the support services proxy server account.
-supportProxyPasswdSecure	Specifies the password in secure mode - the user will be prompted to input the password.
-supportProxyProtocol	Specify the protocol used for communications with the support proxy server. Valid values are: • http • socks --- **Note** Values are case-sensitive. ---
-noSupportProxyUser	Clears support proxy settings.
-autoUpdateContracts	Specify whether the system automatically updates its service contracts list once a week, Valid values are: • yes • no

Qualifier	Description
	Note Values are case-sensitive.

Example

The following command specifies the support services proxy server parameters:

```
uemcli /sys/support/config set -supportProxyAddr 10.0.0.1 -
supportProxyPort 8080 -supportProxyUser user1 -supportProxyPasswd
password123
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage support credentials

Manage support credentials settings on the system, including:

- User name of the user account.
- Password of the user account.

The following table lists the support credentials attributes:

Table 8 Support credentials attributes

Attributes	Description
Support user name	Name of the user account.
Support password	Password of the user account.

View support credentials

View the current support credentials.

Format

```
/sys/support/account show
```

Example

The following command displays the support credentials:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/account
show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      Support user name = user1
```

Change support credentials

Change support credential attributes.

Format

```
/sys/support/account set -user <value> {-passwd <value> | -
passwdSecure}
```

Action qualifiers

Qualifier	Description
-user	Specify the user name of the support account.
-passwd	Specify the new password of the support account.
-passwdSecure	Specifies the password in secure mode - the user will be prompted to input the password.

Example

The following command specifies the new password of the support account:

uemcli /sys/support/account set -user user1 -passwd Password123

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Delete support credentials

Delete support credentials.

Format

```
/sys/support/account delete
```

Example

The following command deletes support credentials:

uemcli /sys/support/account delete

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage support contracts

Manage support contracts on the system.

The following table lists the support contracts attributes:

Table 9 Support contracts attributes

Attributes	Description
ID	Support contract identifier.
Status	State of the support contract. Value is one of the following: • active • about to expire

Table 9 Support contracts attributes (continued)

Attributes	Description
	• expired
Service type	Type of the support contract.
Start date	Start date of the support contract.
Expiration date	Expiration date of the support contract

View support contracts

View the available support contracts.

Format
```
/sys/support/contract [-id <value>] show
```

Action qualifiers

Qualifier	Description
-id	Identifies the support contracts

Example
The following command displays the support contracts:

**uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/
contract show**

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: ID              = contract1
   Status          = active
   Service type    = software
   Expiration date = 2012/12/31
```

Refresh support contracts

Refresh or update the list of support contracts from a support server.

Format
```
/sys/support/contract refresh
```

Example
The following command displays the support contracts:

**uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/
contract refresh**

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage users

Control user access to the system and functionality by creating user accounts for each manager or administrator who needs to configure and monitor the system. The accounts combine a unique username and password with a specific role for each identity. The specified role determines the types of actions that the user can perform after logging in. When users connect to the system through Unisphere CLI or Unisphere, the system prompts them to type their username and password to gain access.

The following table lists the attributes for user roles:

Table 10 User role attributes

Attributes	Description
Name	Name of the user role. Value is one of the following: • `administrator` — Administrator role: Can view system data, edit system settings, and perform all major administrator tasks. • `storageadmin` — Storage administrator role: Can view system data and edit settings. Cannot add user accounts or host configurations, perform initial system configuration, modify network settings, create or delete NAS servers, or upgrade system software. • `operator` — Operator role: Can view system and storage status information but cannot change system settings. This role provides view-only permissions.
Description	Brief description of the user role.

View user roles

View a list of roles to which you can assign users. You can filter on the role name.

Note

The show action command on page 17 explains how to change the output format.

Format
```
/user/role [-name <value>] show
```

Object qualifier

Qualifier	Description
-name	Type the name of the user role. Value is one of the following: • `administrator` — Administrator role • `storageadmin` — Storage Administrator role • `operator` — Operator role (view only)

Example
The following command displays a list of user roles on the system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/role show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection


1:     Name        = administrator
       Description = User is allowed to perform security tasks.

2:     Name         = storageadmin
       Description  = User has access to all administrative and
management interfaces and data.

3:     Name         = operator
       Description = User is allowed to see all storage system data
but not to perform any storage management operations.
```

Create user accounts

Create an account for a user or user group and assign the account to a role. The role specifies the user permissions. Users can be local to the system or authenticated by using LDAP. User groups are only authenticated using LDAP.

Each user account is identified by an ID.

Format
```
/user/account create -name <value> -type {local {-passwd
<value> | -passwdSecure} | ldapuser | ldapgroup} -role <value>
```

Action qualifiers

Qualifier	Description
-name	Type a name for the account. For LDAP users and groups that are required to indicate the domain, use the following format: *<domain>/<name>* where: • *domain* — LDAP domain. • *name* — Account name.
-type	Type the type of user or user group. Value is one of the following: • `local` — Local user. • `ldapuser` — User has an LDAP account. • `ldapgroup` — Group has an LDAP account.
-passwd	For local users, type the user password. The following are the password requirements for user accounts: • Passwords must be 8 to 40 characters in length and cannot contain spaces. • Passwords must include mixed case, a number, and a special character from this list: ! , @ # $ % ^ * ? _ ~ • When changing a password, do not reuse any of the last 3 passwords.

Qualifier	Description
-passwdSecure	Specifies the password in secure mode - the user will be prompted to input the password and the password confirmation.
-role	Type the name of the role for the account. Value is one of the following: • administrator — Administrator • storageadmin — Storage Administrator • operator — Operator (view only) Table 10 on page 37 provides a description of each user role.

Example

The following command creates a user account that assigns user1 as local user to the operator role:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account create

-name user1 -type local -passwd Password987! -role operator

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = user_user1
Operation completed successfully.
```

View user accounts

View a list of user accounts. You can filter on the account ID.

Note

The show action command on page 17 explains how to change the output format.

Format
/user/account [-id <value>] show

Object qualifier

Qualifier	Description
-id	Type the ID of a user account.

Example

The following command displays a list of all user accounts on the system:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:     ID   = user_user1
       Name = user1
       Role = administrator
       Type = local

2:     ID   = ldapuser_ldapdomain.com/ldapUser
```

```
            Name = ldapdomain.com/ldapUser
            Role = operator
            Type = ldapuser

3:      ID   = ldapgroup_ldapdomain.com/ldapGroup
            Name = ldapdomain.com/ldapGroup
            Role = storagadmin
            Type = ldapgroup
```

Change user accounts

Update a user account with new settings.

Format

```
/user/account -id <value> set [ {-passwd <value> | -
passwdSecure} { {-oldpasswd <value> | -oldpasswdSecure} | -
force}] [ -role <value>]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the user account to change.

Action qualifiers

Qualifier	Description
-passwd	Type a new password for a local user. The following are the password requirements for user accounts: • Passwords must be 8 to 40 characters in length and cannot contain spaces. • Passwords must include mixed case, a number, and a special character from this list: ! , @ # $ % ^ * ? _ ~ • When changing a password, do not reuse any of the last 3 passwords.
-passwdSecure	Specifies the password in secure mode - the user will be prompted to input the password and the password confirmation.
-oldpasswd	Type the old password to set the new password.
-oldpasswdSecure	Specifies the password in secure mode - the user will be prompted to input the password.
-force	Reset the password. **Note** You must be an administrator to use this qualifier.
-role	Type the name of a new role for the account. Value is one of the following: • administrator — Administrator • storageadmin — Storage Administrator

Qualifier	Description
	• `operator` — Operator (view only) Table 10 on page 37 provides a description of each user role.

Example

The following command changes the password for user account user_user1:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account -id`
`user_user1 set -passwd NewPassword456! -oldpasswd OldPassword456!`

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = user_user1
Operation completed successfully.
```

Delete user accounts

Delete a user account.

Format
`/user/account -id <value> delete`

Object qualifier

Qualifier	Description
`-id`	Type the ID of the user account to delete.

Example

The following command deletes user account user_user1:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account -id`
`user_user1 delete`

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully
```

View installed feature licenses

View details for purchased feature licenses. These licenses were purchased when your system was purchased. You must install licenses on your system before you can use a particular feature or perform tasks, such as creating storage.

To install a license, use the `-upload` switch to upload it to the system. View the switches on page 346 provides details on all available switches. The following table lists and describes the attributes for product licenses.

Table 11 License attributes

Attribute	Description
`Feature`	Name of the feature.
`Installed`	Indication of whether a feature is installed with the license. Value is yes or no.
`Version`	Version of the license.
`Issued`	Date when the license was made available.
`Expires`	Date when the license will expire.
`Health state`	Health state of the license. The health code appears in parentheses. Value is one of the following: • `OK (5)` — License is active. • `Degraded/Warning (10)` — License will soon expire. • `Major failure (20)` — License has expired. To update a license that has expired or is about to expire, go to the **Manage Licenses** page in Unisphere.
`Health details`	Additional health information. See Appendix A, Reference on page 367, for health information details.

View licenses

View details about installed licenses.

Note

The show action command on page 17 explains how to change the output format.

Format
`/sys/lic show`

Example
The following command displays a list of all feature licenses on the system:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/lic show

```
1:      Feature      = ISCSI
        Installed    = yes
        Version      = 1.1
        Issued       = 2009-11-09
        Expires      = 2010-11-09
        Health state = OK (5)

2:      Feature      = CIFS
        Installed    = yes
        Version      = 1.1
        Issued       = 2009-01-19
        Expires      = Never
        Health state = OK (5)
```

View and accept the End User License Agreement

View the end user license agreement (EULA). You must accept the EULA prior to uploading product licenses or configuring the system.

View the EULA

View the EULA as a text file. The output displays a URL for accessing the text file.

Note

explains how to change the output format.

Format
```
/sys/eula show
```

Example
The following command displays the agreement status of the EULA and a URL for viewing the EULA as a text file:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/eula show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:     Agree = yes
       URL   = https:/10.0.0.1/eula.txt
```

Accept the EULA

Accept the EULA prior to install product licenses and configure the system.

Format
```
/sys/eula set -agree yes
```

Example
The following command accepts the EULA:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/eula set -agree yes

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage ESRS (if supported)

EMC Secure Remote Support (ESRS) is a feature that provides EMC with remote access capabilities to systems in the field through a secure and encrypted tunnel.

The following table lists the ESRS attributes:

Table 12 ESRS attributes

Attributes	Description
ESRS enabled	Indicates whether the ESRS service is enabled. The proxy server and policy manager must be set in order to enable the ESRS service.
ESRS connection status	Status of the connection to the ESRS server. Value is one of the following: • Connected • Not connected • Disabled • Not running
Policy manager	Policy manager name or IP address.
Policy manager port	Policy manager port number.
Policy manager protocol	Protocol used for communications with the policy manager. Value is one of the following: • http • https (default) **Note** Values are case-sensitive.
Policy proxy server address	Name or IP address of the proxy server used by the policy manager.
Policy proxy server port	Port of the proxy server used by the policy manager.
Policy proxy user name	User name of the account on the policy proxy server.
Policy proxy user password	Password of the account on the policy proxy server.
Policy proxy protocol	The protocol used for communications with the policy proxy server. Valid values are: • http • socks (default) **Note** Values are case-sensitive.

View ESRS configuration

View details about the ESRS configuration.

Format
```
/sys/support/esrs show
```

Example

The following command displays the ESRS configuration:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrs show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: ESRS enabled                 = yes
   ESRS connection status       = active
   Policy manager address       = 10.10.0.2
   Policy manager port          =
   Policy proxy server address  = 10.0.0.3
   Policy proxy server port     = 8080
```

Change ESRS configuration

Modify the ESRS configuration.

Note

Valid EMC support credentials must be set in order to execute this command. Policy manager address and policy proxy address must be configured or specified in the command in order to modify other policy manager or proxy parameters.

Format

```
/sys/support/esrs set [-enable {yes | no}] { [-
policyManagerAddr <value>] [ -policyManagerProtocol {http |
https}] [ -policyManagerPort <value>] [ -policyProxyAddr
<value>] [ -policyProxyProtocol { socks | http }] [ -
policyProxyPort <value>] [-policyProxyUser <value> {-
policyProxyPasswd <value> | -policyProxyPasswdSecure} ] | -
noPolicyManager} [-pingRate high]
```

Action qualifiers

Qualifier	Description
–enable	Specifies whether to enable or disable the ESRS. Possible values include: • yes • no --- **Note** Values are case-sensitive.
–policyManagerAddr	Specifies the name or IP address of the policy manager.
–policyManagerProtocol	Specifies the protocol used for communications with the policy manager. Possible values include: • http • https (default)

Qualifier	Description
	Note Values are case-sensitive.
`-policyManagerPort`	Specifies the policy manager port number.
`-policyProxyAddr`	Specifies the name or IP address of the proxy server used by the policy manager.
`-policyProxyProtocol`	Specifies the protocol used for communications with the policy proxy server. Valid values are: • `http` • `socks`(default) **Note** Values are case-sensitive.
`-policyProxyPort`	Specifies the port number of the policy proxy server.
`-policyProxyUser`	Specifies the user name of the account on policy proxy server.
`-policyProxyPasswd`	Specifies the password of the account on policy proxy server.
`-policyProxyPasswdSecure`	Specifies the password in secure mode - the user will be prompted to input the password.
`-noPolicyManager`	Clears policy manager and policy proxy settings.
`-pingRate`	Specifies to increase the ping rate for a period of time. Value is: • `high` **Note** Values are case-sensitive.

Example
The following command modifies the ESRS configuration:

uemcli /sys/support/esrs set -enable yes –policyManagerAddr 10.10.0.2 -policyManagerPort 8090 –policyManagerProtocol https –policyProxyAddr 10.0.0.3 -policyProxyPort 8080 –policyProxyUser user2 – policyProxyPasswd password456 –policyProxyProtocol http

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage Unisphere Central Management/Monitoring

Unisphere Central management/monitoring is a centralized approach to monitoring multiple systems at one time.

The following table lists the Unisphere Central management/monitoring attributes:

Table 13 Unisphere Central management/monitoring attributes

Attribute	Description
ID	Unisphere Central management server identifier.
Address	Unisphere Central management server network address (network name or IP address)
Certificate	Unisphere Central management server certificate SHA1 hash.
Challenge phrase	Passphrase used by the Unisphere Central management server to sign a certificate.
SSO enabled	Indicates whether the system uses the remote manager as the authentication server. Value is one of the following: • Yes • No

Create the remote manager configuration

Format
```
/sys/ur create -addr <value> { -certificate <value> -passphrase
<value> | -unsecured }
```

Action qualifiers

Qualifier	Description
-addr	Specifies the Unisphere Central management server name or IP address.
-certificate	Specifies the hash of the existing certificate.
-passphrase	Specifies the challenge phrase for the Unisphere Central manager to sign the certificate.
-unsecured	Skips certificate and challenge phrase.

Example
```
uemcli /sys/ur create -addr 10.10.0.1 -certificate
2fd4e1c67a2d28fced849ee1bb76e7391b93eb12 -passphrase password


Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = ur_0
```

```
Operation completed successfully.
```

View remote manager configuration

Displays the remote manager configuration.

Format
`/sys/ur show`

Example
The following command displays the Unisphere Central manager configuration:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/ur show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: ID      = ur_0
   Address = 10.10.0.2
```

Change remote manager configuration

Update a user account with new settings.

Format
`/sys/ur [-id <value>] set [-addr <value>] [ {-certificate <value> {-passphrase <value> | -passphraseSecure} | -unsecured} ] [-ssoEnabled {yes | no}]`

Object qualifier

Qualifier	Description
-id	Identifies the Unisphere Central management server. Optional if there is only one remote manager configured.

Action qualifiers

Qualifier	Description
-addr	Specify the Unisphere Central management server name or IP address.
-certificate	Specify the hash of existing certificate.
-passphrase	Specify the challenge phrase for the remote manager to sign the certificate.
-passphraseSecure	Specifies the challenge phrase in secure mode - the user will be prompted to input the challenge phrase.
-unsecured	Skip certificate and challenge phrase.
-ssoEnabled	Specify whether you want to set the remote manager as the authentication server for the local system. Valid values are yes or no. The default value is set to no, which indicates that the authentication server is the local system.

Example

```
uemcli /sys/ur set -addr 10.10.0.2
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage remote logging

Log system messages to a remote host. Create a setting for remote logging that specifies the following:

- The facility that will generate the log messages.

- The network name or IP address of a remote host that will receive the log data.

The remote host must be accessible from the system. Security for the log information must be provided through network access controls or the system security at the remote host. You can configure the log transmission method (UDP or TCP) and the host port that the system uses. By default, the system transfers log information on port 515 over the UDP protocol.

Log files record messages to flat log files. The user-level system messages are recorded in English. However, you can specify a facility to select the type of information contained in the logs, according to the system component that issues it, and the language of any text in the log.

explains viewing details about current logs and alerts on the system.

The following table lists the attributes for remote system logging.

Table 14 Remote logging attributes

Attribute	Description
Enabled	Indication of whether remote logging is currently enabled. Value is yes or no.
Host	IP address or network name of the remote host.
Port	Port number on the remote host. Default is 515.
Protocol	Protocol for transferring the log. Value is TCP or UDP.
Facility	Facility that will process the log. Value is one of the following: • KERN — Kernel messages. • USER — User-level messages. • MAIL — Mail system. • DAEMON — System daemons. • AUTH — Security/authorization messages. • Syslog — Message generated internally by syslogd (default). • LPR — Line printer subsystem. • NEWS — Network news subsystem. • UUCP — UNIX-to-UNIX copy.

Table 14 Remote logging attributes (continued)

Attribute	Description
	• `CRON` — Clock daemon. • `AUTHPRIV` — Security/authorization messages. • `FTP` — FTP daemon.

View settings for remote logging

View remote logging settings.

Note

explains how to change the output format.

Format
```
/sys/rlog show
```

Example
The following command displays the settings for remote system logging:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/rlog show`

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      Enabled  = yes
        Host     = 10.64.75.201
        Port     = 500
        Protocol = UDP
        Facility = Kernel messages
```

Configure settings for remote logging

Configure for remote logging.

Format
```
/sys/rlog set [-enabled {yes|no}] [-host <value>] [-port
<value>] [-protocol {UDP|TCP}] [-facility {KERN|USER|MAIL|
DAEMON|AUTH|Syslog|LPR|NEWS|UUCP|CRON|AUTHPRIV|FTP}]
```

Object qualifier

Qualifier	Description
`-enabled`	Specify to enable remote system logging. Value is yes or no. If you specify yes, include `-host <value>`, where value is the IP address of the target remote host that will receive the logs.
`-host`	Type the IP address or network name of the remote host that will receive the log files. Value is one of the following: • `IPv4` • `IPv6` • `Network name`

Qualifier	Description
`-port`	Type the port number on the remote host. Default is 515.
`-protocol`	Type the protocol for transferring the log files. Value is TCP or UDP.
`-facility`	Type the facility that will process the log files. Value is one of the following: • `KERN` — Kernel messages. • `USER` — User-level messages. • `MAIL` — Mail system. • `DAEMON` — System daemons. • `AUTH` — Security/authorization messages. • `Syslog` — Message generated internally by syslogd (default). • `LPR` — Line printer subsystem. • `NEWS` — Network news subsystem. • `UUCP` — UNIX-to-UNIX copy. • `CRON` — Clock daemon. • `AUTHPRIV` — Security/authorization messages. • `FTP` — FTP daemon.

Example

The following command configures remote system logging with these settings:

- Remote target host is 10.64.74.12
- Uses host port 500.
- Uses protocol UDP.
- Uses the MAIL facility.

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/rlog set -`
`enabled yes -host 10.64.74.12 -port 500 -protocol UDP -facility MAIL`

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

View system software versions

Display details about the version of the installed system software and the software upgrade candidate that has been uploaded to the system. Upgrade the system software on page 53 explains how to upgrade the system software. The following table lists the system software attributes.

Table 15 System software attributes

Attribute	Description
ID	ID of the system software.
Type	System software type. Value is one of the following: • `installed` — System software that is currently installed on the system. • `candidate` — Upgrade candidate uploaded to the system for upgrading the system software.
Version	Software version.
Release date	Software release date.
Image filename	Filename of the software image.

Note

The show action command on page 17 explains how to change the output format.

Format
```
/sys/soft/ver [{-id <value>|-type {installed|candidate}}] show
```

Object qualifier

Qualifier	Description
-id	Type the ID of the system software.
-type	Type the software type. Value is one of the following: • `installed` — View the version of the system software that is installed. • `candidate` — View the version of the system software upgrade candidate that was uploaded to the system. **Note** Values are case-insensitive.

Example
The following command displays details about the installed system software and an uploaded upgrade candidate:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/soft/ver show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID           = INST_1
        Type         = installed
        Version      = 0.1.0.1487
        Release date = 2009-04-30

2:      ID           = CAND_1
        Type         = candidate
```

```
        Version     = 0.1.0.2187
        Release date = 2009-11-14
```

Upgrade the system software

Create an upgrade session to upgrade the system software or view existing upgrade sessions. The upgrade session installs an upgrade candidate file that was uploaded to the system. Download the latest upgrade candidate from the support website. Use the - upload switch to upload it to the system before creating the upgrade session. View the switches on page 346 provides details for all available switches.

The latest software upgrade candidate contains all available hot fixes. If you have applied hot fixes to your system, the hot fixes will be included in the latest upgrade candidate.

Note

All system components must be healthy, prior to upgrading the system software. If any system components are degraded, the software update will fail. Perform a system health check on page 27 explains how to run a health check on the system.

The following table lists the attributes for upgrade sessions.

Table 16 Upgrade session attributes

Attribute	Description
Status	Current status of the upgrade session. Value is one of the following: • running — Session is upgrading the system software. • completed — Session has completed upgrading the system software. • failed — Upgrade session has failed.
Progress	Current progress of the upgrade session.
Creation time	Date and time when the upgrade session was created.
Elapsed time	Amount of time that the upgrade session has been running.
Estimated time left	Estimated time required to complete the upgrade session.

Create upgrade sessions

Create a session to upgrade the system software with an uploaded upgrade candidate.

⚠ **CAUTION**

Do not use Unisphere or Unisphere CLI to manage or configure the system during a software upgrade.

Format
```
/sys/soft/upgrade create -candId <value>
```

Action qualifiers

Qualifier	Description
`-candId`	Type the ID of the uploaded upgrade candidate. View system software versions on page 51 explains how to view the ID of the uploaded software candidate.

Example

The following command creates a session to upgrade the system software to upgrade candidate CAND_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/soft/upgrade create -candId CAND_1

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = UPGSES_1
Operation completed successfully.
```

Note

All warning messages, if any, appear the first time you run the upgrade process. When a potential issue results in a warning message, the upgrade process stops. Once you review the warning message, run the upgrade command again to continue with the upgrade process. This time the upgrade process will run the checks again, but it will not stop for any warnings. The upgrade process will only stop when an error occurs.

View upgrade sessions

View details for an existing software upgrade session.

Note

The show action command on page 17 explains how to change the output format.

Format
`/sys/soft/upgrade show`

Example

The following command displays details about the system software upgrade session:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/soft/upgrade show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:     Status              = Running
       Status message      =
       Creation time       = 2009-11-09 19:43:08
       Elapsed time        = 01h 43m 08s
       Estimated time left = 01h 10m 00s
       Progress            = Task 5 of 25 (Stopping c4 stack on SPA)
       Percent complete    = 15%

2:     Status              = Failed
```

```
Status message       = Stopping c4 stack on SPA timeout expired
Creation time        = 2009-11-09 18:04:12
Elapsed time         = 00h 20m 08s
Estimated time left =
Progress             = Task 5 of 25 (Stopping c4 stack on SPA)
Percent complete     = 15%
```

Manage snapshot protection schedules

To schedule snapshot creation, you assign a protection schedule to the storage resource of which to take snapshots. Schedules contain one or more task rules that define the time and frequency when snapshots of the storage resource are taken. When you create a task rule you can assign it to an existing schedule or the system will automatically assign it to a new schedule. Manage task rules on page 56 explains how to set up task rules. Manage snapshots on page 278 explains how to create snapshots manually and manage existing snapshots.

Each protection schedule is identified by an ID.

The following table lists the attributes for protection schedules.

Table 17 Protection schedule attributes

Attribute	Description
ID	ID of the schedule.
Name	Name of the schedule.
Type	Type of schedule. Value is one of the following: • System — Defined by the system. • User — Defined by a user.
Rules	List of IDs for each task rule in the schedule. Manage task rules on page 56 provides details about schedule rules.

View protection schedules

View details about protection schedules. You can filter on the schedule ID.

Note

The show action command on page 17 explains how to change the output format.

Format
`/sys/task/sched [-id <value>] show`

Object qualifier

Qualifier	Description
-id	Type the ID of a schedule.

Example
The following command displays details about all schedules (user- and system-defined) on the system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/sched show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID    = LessProtectionID
        Name  = Less Protection
        Type  = System
        Rules = RULE_1, RULE2

2:      ID    = DefaultProtectionID
        Name  = Default Protection
        Type  = System
        Rules = RULE_3


3:      ID    = MySchedID
        Name  = MySched1
        Type  = User
        Rules = RULE_4
```

Delete protection schedules

Delete a user-defined protection schedule. You cannot delete a system-defined schedule.

Note

When you delete a schedule, all rules associated with the schedule are also deleted.

Format
```
/sys/task/sched [-id <value>] delete
```

Object qualifier

Qualifier	Description
-id	Type the ID of the schedule to delete.

Example
The following command deletes schedule MySchedID:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/sched -id
MySchedID delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage task rules

Task rules define the time and frequency when a task, such as snapshot creation, will occur. When you create a task rule, you can assign it to an existing protection schedule or the system automatically assigns it to a new schedule. You then assign the schedule to the storage resource of which to schedule snapshots. Manage snapshot protection schedules on page 55 explains how to view and delete protection schedules.

The following table lists the attributes for task rules.

Table 18 Task rule attributes

Attribute	Description
ID	ID of the rule.
Type	Type of rule, which specifies when a task executes. Value is one of the following: • HoursInterval — Task executes on an interval of the specified number of hours or minutes within an hour. • HoursList — Task executes everyday on the specified hours and, optionally, on a specific minute within the specified hour. • DaysInterval — Task executes on an interval of the specified number of days and, optionally, on a specific hour of each specified day. • WeekDaysList — Task executes on the specified days of the week or on a specific hour of each specified day. • MonthDaysList — Task executes each month on a specified day and time.
Frequency	Frequency that a task executes.
Keep for	For snapshots, the amount of time the system retains a snapshot before deleting it.
Allow auto-delete	For snapshots, indicates whether the snapshot can be deleted automatically. Value is one of the following: • Yes — The system can delete the snapshot automatically. • No — The system cannot delete the snapshot automatically.
Access	For snapshots, indicates whether the snapshot created by this schedule is a checkpoint, or is set to read/write. Value is one of the following: • Ckpt — The snapshot is a read-only checkpoint • Share — The snapshot is set to read/write for users to create CIFS shares of NFS exports.

Create task rules

Create a task rule.

Format
```
/sys/task/rule create {-schedId <value>|-schedName <value>} -
type {HoursInterval -every <value> [-at <value>]|HoursList -
hours <value> [-at <value>]|DaysInterval -every <value> [-at
<value>]|WeekDaysList -days <value> [-at <value>]|MonthDaysList
-days <value> [-at <value>]} [{-keepFor <value> |-
allowAutoDelete {yes|no}}] [-access {ckpt|share}]
```

Action qualifiers

Qualifier	Description
-schedId	Type the ID of an existing protection schedule to which to assign the rule. View protection schedules on page 55 explains viewing details about existing schedules, including their IDs.
-schedName	Type a name for a new protection schedule to which to assign the rule.
-type	Specify the type of rule, which indicates how often the task will execute. Value is one of the following: • HoursInterval — Task executes on an interval of the specified number of hours or minutes within an hour. • HoursList — Task executes everyday on the specified hours and, optionally, on a specific minute within the specified hour. • DaysInterval — Task executes on an interval of the specified number of days and, optionally, on a specific hour of each specified day. • WeekDaysList — Task executes on the specified days of the week or on a specific hour of each specified day. • MonthDaysList — Task executes each month on a specified day and time.
-every	If the value of -type is HoursInterval or DaysInterval, type the time interval when the task will execute. Value is one of the following: • HoursInterval — Number of hours within the range 1–24. • DaysInterval — Number of days within the range 1–31.
-hours	If the value of -type is HoursList, type a comma-separated list of the hours of the day when the task will execute. The range is 0–23.
-at	Type the specific number of minutes of an hour and the minutes of a day when the task will execute based on the value of -type. Value is one of the following: • HoursInterval or HoursList — Type the number of minutes after the hour within the range 0–59. Default is 0. • DaysInterval, WeekDaysList, or MonthDaysList — Type the time of a day in the following format: ‹*HH*›[:*MM*] where *HH* is the hour of the day and *MM* represents the minutes within the specified hour. Value range is 0:00–23:59. Default value is 0:00.
-days	If the value of -type is WeekDaysList or MonthDaysList, type the days of the week or the day of the month when the task will execute:

Qualifier	Description
	• `WeekDaysList`—Type a comma-separated list of the days of the week. Value is one of the following: ▪ `Mon` — Monday ▪ `Tue` — Tuesday ▪ `Wed` — Wednesday ▪ `Thu` — Thursday ▪ `Fri` — Friday ▪ `Sat` — Saturday ▪ `Sun` — Sunday • `MonthDaysList` — Type the day of the month within the range 1–31. **Note** Values are case-insensitive. For MonthDaysList, you can specify only 1 day of the month.
`-keepFor`	Type the number of days or hours the system will retain a snapshot before deleting it. Use the following format: ‹*value*›[‹*qualifier*›] where: • *value* — Type the number of hours or days. Value is: ▪ `Hours` — Number of hours within the range 1–24. ▪ `Days` — Number of days within the range 1–31. • *qualifier* — Type the value qualifier. Value is one of the following: ▪ `h` — Indicates hours. ▪ `d` — Indicates days. Default value is 1h (1 hour).
`-allowAutoDelete`	Specify whether the system can automatically delete the snapshot or snapshot set. Value is one of the following: • `Yes` (default) • `No`
`-access`	Specify whether the snapshot is a read-only checkpoint, or read/write for CIFs shares or NFS exports. Value is one of the following: • `ckpt` (default) • `share`

Example 1

The following command creates a task rule with these settings:

• Assigns the rule to the new protection schedule MyScheduleID.

- Takes a snapshot every 12 hours and 30 minutes.

- Keeps the snapshot for 10 hours before deleting it:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/rule
create –schedName MyScheduleID -type HoursInterval -every 12 –at 30 –
keepFor 10h
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = RULE_1
Schedule ID = MyScheduleID
Operation completed successfully.
```

Example 2

The following command creates a task rule with these settings:

- Assigns the rule to the existing protection schedule MySchedID.

- Takes a snapshot everyday at 12:30 a.m., 8:30 a.m., and 8:30 p.m.:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/rule
create –schedId MySchedID -type HoursList –hours "0,8,20" –at 30
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = RULE_2
Operation completed successfully.
```

Example 3

The following command creates a task rule with these settings:

- Assigns the rule to the existing protection schedule MySchedID.

- Takes a snapshot every 2 days at 1:20 p.m.

- Keeps the snapshot for 1 week (7 days) before deleting it:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/rule
create –schedId MySchedID -type DaysInterval -every 2 –at 13:20 –
keepFor 7d
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = RULE_3
Operation completed successfully.
```

Example 4

The following command creates a task rule with these settings:

- Assigns the rule to the existing protection schedule MySchedID.

- Takes a snapshot every Monday, Wednesday, and Friday at 6 a.m.:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/rule
create –schedId MySchedID -type WeekDaysList -days "Mon,Wed,Fri" –at 6
```

```
Storage system address: 10.0.0.1
Storage system port: 443
```

```
HTTPS connection

ID = RULE_4
Operation completed successfully.
```

Example 5

The following command creates a task rule with these settings:

- Assigns the rule to the existing protection schedule MySchedID.

- Takes a snapshot on the first day of every month at 12 p.m.:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/rule
create –schedId MySchedID -type MonthDaysList -days 1

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = RULE_5
Operation completed successfully.
```

View task rules

View details about task rules. You can filter on the ID of a rule or type the ID of a protection schedule to view only the rules assigned to that schedule.

Note

The show action command on page 17 explains how to change the output format.

Format
`/sys/task/rule [{-id <value> | –sched<value>}] show`

Object qualifier

Qualifier	Description
-id	Type the ID of a rule.
-sched	Type the ID of a protection schedule to view the rules associated with it.

Example

The following command lists details for all task rules assigned to protection schedule SCHD_3:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/rule –
sched SCHD_3 show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID        = RULE_1
        Type      = HoursInterval
        Frequency = Every 12h at 30m after the hour
        Keep for  = 10h

2:      ID        = RULE_2
        Type      = HoursList
        Frequency = Every day at 0:20, 8:20, 20:20
        Keep for  = 1h
```

```
3:      ID        = RULE_3
        Type      = DaysInterval
        Frequency = Every 2d at 13:20
        Keep for  = 7d

4:      ID        = RULE_4
        Type      = WeekDaysList
        Frequency = Every Mon, Wed, Fri at 6:00
        Keep for  = 1h

5:      ID        = RULE_5
        Type      = MonthDaysList
        Frequency = Every 1st, 2nd, 3rd day of month at 0:00
        Keep for  = 1h
```

Delete task rules

Delete a task rule.

Note

You cannot delete a rule that is associated with a system-defined schedule, only a user-defined schedule. Also, when you delete the last rule in a schedule, the schedule is also deleted.

Format
`/sys/task/rule -id <value> delete`

Object qualifier

Qualifier	Description
-id	Type the ID of the rule to delete.

Example
The following command deletes rule RULE_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/rule -id RULE_1 delete

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage jobs

Manage the operations that are running in the background.

The following table lists the attributes for jobs.

Table 19 Jobs attributes

Attribute	Description
ID	Job identifier.
Type	Job type. Value is one of the following:

Table 19 Jobs attributes (continued)

Attribute	Description
	`Provisioning` `Snapshot` `Snapshot schedule`
`Title`	Job title.
`State`	Job state. Value is one of the following: `Queued` `Running` `Suspended` `Completed` `Completed with problems` `Failed` `Rolling back`
`Step`	Current step.
`User`	User who started the job.
`Start time`	Time when the job was started.
`Elapsed time`	Elapsed time for the current job.
`Estimated time left`	Time remaining to complete the current job.
`Percent complete`	Job progress in percent.

View list of jobs

View the list of existing jobs.

Format
```
sys/task/job [{ -id <value> | -active | -failed | -completed }]
show
```

Object qualifier

Qualifier	Description
`-id`	Identifies the job.
`-active`	Show only unfinished jobs (Queued, Running, Suspended, Rolling back).
`-failed`	Show only failed jobs.
`-completed`	Show only successfully completed and completed with problems jobs.

Example
The following command displays a list of all jobs:

```
uemcli /sys/task/job show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:     ID                    = N-26
       Type                  = Provisioning
       Title                 = Create or modify storage resource
       State                 = Completed
       Step                  = 2 of 2 (Apply iSCSI hosts)
       Percent complete      = 100%
```

Resume a job

Resumes an existing job. Could be applied to the suspended job only.

Format
`/sys/task/job –id <value> resume`

Object qualifier

Qualifier	Description
–id	Identifies the job.

Example
The following command resumes an existing job.

```
uemcli /sys/task/job -id N-23564 resume
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Cancel a job

Cancels an existing job without rolling back. Could be applied to the suspended or queued job only.

Format
`sys/task/job –id <value> cancel`

Object qualifier

Qualifier	Description
–id	Identifies the job.

Example
The following command resumes an existing job.

```
uemcli /sys/task/job -id N-23654 cancel
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Delete jobs

Deletes a job or a group of jobs. Active jobs cannot be deleted.

Format
```
sys/task/job { -id <value> | -failed | -completed } delete
```

Object qualifier

Qualifier	Description
`-id`	Identifies the job.
`-failed`	Identifies jobs that have failed.
`-completed`	Identifies jobs that have completed successfully or completed with problems.

Example
The following command deletes an existing job.

uemcli /sys/task/job -id N-23654 delete

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage job step

Manage the steps of the specified job.

The following table lists the attributes for job step.

Table 20 Job step attributes

Attribute	Description
`Title`	Step title.
`Status`	Step status. Value is one of the following: • `Queued` • `Running` • `Completed` • `Failed`
`Execution result code`	The error code of the operation.
`Execution result description`	The error message of the operation.
`Rollback result code`	The error code of the rollback.

Table 20 Job step attributes (continued)

Attribute	Description
`Rollback result description`	The error message of the rollback.
`Details`	Additional information. Format: key: "value", key: "value",..

View list of steps in a job

Displays a list of steps of the specified job.

Format

```
sys/task/job/step -jobId <value> show
```

Object qualifier

Qualifier	Description
`-jobId`	Identifies the job.

Example

The following command displays a list of steps of the specified job

`uemcli /sys/task/job/step -jobId N-23654 show`

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:  Title                        = Extend storage pool
    Status                       = Completed
    Execution result code        = 0
    Execution result description =
    Rollback result code         = 0
    Rollback result description  =
    Details                      = ID: "local_pool_8"; Name: "SASx6_2"

2:  Title                        = Create application
    Status                       = Completed
    Execution result code        = 0
    Execution result description =
    Rollback result code         = 0
    Rollback result description  =
    Details                      = ID: "local_pool_8"; Name: "SASx6_2"

3:  Title                        = Create file system
    Status                       = Running
    Execution result code        = 0
    Execution result description =
    Rollback result code         = 0
    Rollback result description  =
    Details                      = ID: fs_99; Name: JobTest11

4:  Title                        = Create NFS share
    Status                       = Queued
    Execution result code        = 0
    Execution result description =
    Rollback result code         = 0
    Rollback result description  =
    Details                      = ID: nfs_45; Name: JobTest11
```

```
5:  Title                        = Finalize allocation
    Status                       = Queued
    Execution result code        = 0
    Execution result description =
    Rollback result code         = 0
    Rollback result description  =
    Details                      = ID: local_pool_8; Name: SASx6_2
```

CHAPTER 3

Configure Network Communication

This chapter addresses the following topics:

Manage NAS servers

NAS servers are software components on the system that are dedicated to managing operations for data transferred through the CIFS or NFS protocols. You must configure at least one NAS server before you can create network share storage. You can configure a NAS server to support Windows network shares (CIFS), Linux/UNIX network shares (NFS), or both.

NAS servers run on each SP and communicate with network hosts through SP ports. Once you configure a NAS server, you can then create file systems from which you export NFS or CIFS network shares. Configured hosts map or mount the network shares to access the file system storage.

Each NAS server is identified by an ID.

The following table lists the attributes for NAS servers.

Table 21 NAS server attributes

Attributes	Description
ID	ID of the NAS server.
Name	Name of the NAS server.
Health state	Health state of the NAS server. The health state code appears in parentheses. Value is one of the following: • `Unknown (0)` — Status is unknown. • `OK (5)` — Working correctly. • `OK BUT (7)` — Configuration is not complete. • `Degraded/Warning (10)` — Working and performing all functions, but the performance may not be optimum. • `Minor failure (15)` — NAS server has faulted. • `Major failure (25)` — Failed and recovery may not be possible. This condition has resulted in data loss and should be remedied immediately.
Health details	Additional health information. See Appendix A, Reference, for details.
SP	Primary SP on which the NAS server runs. **Note** If the primary SP is degraded or has failed, the server fails over to the other SP. The value displays the current SP the server is using in parentheses. For example, SPA (failed over to SPB).
Storage pool	Associated storage pool identifier.
Interface	ID of the network interface assigned to the NAS server that defines the server IP address and allows the server to communicate with the network and hosts. Manage interfaces on page 104 explains how to configure network interfaces on the system.

Table 21 NAS server attributes (continued)

Attributes	Description
	Note It is allowable to remove the last interface of the server.
NFS enabled	Indicates whether NFSv3 file systems are enabled on the NAS server. NFS file systems provide support for NFS network shares. Valid values are: • `Yes` (default) • `No`
NFSv4 enabled	Indicates whether NFS shares can be accessed using the NFSv4 protocol. Valid values are: • `Yes` • `No` (default) **Note** A value of yes will enable both the NFSv3 and NFSv4 protocols.
CIFS enabled	Indicates whether CIFS file systems are enabled on the NAS server. Value is yes or no. Default is no. CIFS file systems provide support for CIFS network shares.
Multiprotocol sharing enabled	Indicates whether multiprotocol sharing is enabled for all file systems on the NAS server. Valid values are: • `Yes` • `No`
Unix directory service	Directory service used for looking up identity information for Unix such as UIDs, GIDs, net groups, and so on. Valid values are: • `nis` • `ldap` • `none` (default) **Note** A value other than the default is required for accurate multiprotocol files sharing between Unix and Windows users.
Default Unix username	Default Unix user name that grants file access in the multiprotocol sharing mode. This user name is used when the corresponding Unix/ Linux user name is not found by the mapping mechanism.
Default Windows username	Default Windows user name that grants file access in the multiprotocol sharing mode. This user name is used when the corresponding Windows user name is not found by the mapping mechanism.
Extended Unix credentials enabled	Indicates whether there are more than 16 Unix groups. Valid values are yes or no (default).

Table 21 NAS server attributes (continued)

Attributes	Description
Credentials cache retention	The amount of time (in minutes) when the credential cache refreshes or times out. Default value is 15 minutes.

Create NAS servers

Create a NAS server. You can create a maximum of 24 NAS servers per system.

Format

```
/net/nas/server create -name <value> -sp <value> -pool <value>
[{-enableNFS {yes | no} | -enableNFSv4 {yes | no}}] [-
mpSharingEnabled {no | yes [-unixDirectoryService {ldap | nis |
none}] [-defaultUnixUser <value>] [-defaultWindowsUser
<value>]}] [-extendedUnixCredEnabled {yes|no}] [-
credCacheRetention <value>]
```

Action qualifiers

Qualifier	Description
-name	Type a name for the NAS server. **Note** Note: NAS server names can contain alphanumeric characters, a single dash, and a single underscore. Server names cannot contain spaces or begin or end with a dash. You can create NAS server names in four parts that are separated by periods (example: aa.bb.cc.dd). Names can contain up to 255 characters, but the first part of the name (before the first period) is limited to 15 characters.
-sp	Specifies the parent SP for the NAS server.
-pool	Specifies the ID of the storage pool for the NAS server.
-enableNFS	Enables NFSv3 file systems on the NAS server. Valid value are: • `yes` (default) • `no`
-enableNFSv4	Specifies whether NFS shares can be accessed using the NFSv4 protocol. Valid values are (case insensitive): • `yes` • `no` (default)

Qualifier	Description
	Note NFSv3 file systems are also enabled when the NFSv4 protocol is enabled.
`-mpSharingEnabled`	Indicates whether multiprotocol sharing mode is enabled. Valid values are: • `yes` • `no` (default)
`-unixDirectoryService`	Directory Service used for querying identity information for Unix (such as UIDs, GIDs, net groups). Valid values are: • `nis` • `ldap` • `none` (default)
`-defaultUnixUser`	Default Unix user name that grants file access in the multiprotocol sharing mode. This user name is used when the corresponding Unix/Linux user name is not found by the mapping mechanism.
`-defaultWindowsUser`	Default Windows user name that grants file access in the multiprotocol sharing mode. This user name is used when the corresponding Windows user name is not found by the mapping mechanism.
`-extendedUnixCredEnabled`	Specifies whether there are more than 16 Unix groups. Valid values are yes or no (default).
`-credCacheRetention`	Specifies the amount of time (in minutes) when the credential cache refreshes or times out. Default value is 15 minutes.

Example

The following command creates a NAS server with these settings:

• Name is nas_1.

• Associated to SP A.

• Associated to storage pool pool_0.

• Supports NFS file systems.

• The server receives the ID nas_1.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server
create -name nas_1 -sp spa -pool pool_0 -enableNFS yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = nas_1
Operation completed successfully.
```

View NAS servers

View details about configured NAS servers, including their name, ID, and whether they have enabled support for CIFS file systems or NFS file systems. You can filter on the NAS server ID.

Note

The show action command on page 17 explains how to change the output format.

Format

/net/nas/server [-id *<value>*] show

Object qualifier

Qualifier	Description
-id	Type the ID of a NAS server.

Example

The following command displays a list of all configured NAS servers:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection


1:     ID                          = nas_1
       Name                        = MyFS1
       NetBIOS name                = MyFS1
       SP                          = spa
       Storage pool                = pool_0
       Interface                   = if_0,if_1
       NFS enabled                 = yes
       NFSv4 enabled               = no
       CIFS enabled                = no
       Multiprotocol sharing enabled = no
       Unix directory service      = none
       Health state enabled        = OK_BUT (7)

2:     ID                          = nas_2
       Name                        = MyFS2
       NetBIOS name                = MyFS2
       SP                          = spa
       Storage pool                = pool_1
       Interface                   = if_3
       NFS enabled                 = yes
       NFSv4 enabled               = no
       CIFS enabled                = yes
       Multiprotocol sharing enabled = yes
       Unix directory service      = ldap
       Health state                = OK (5)
```

Change NAS server settings

Modify an existing NAS server.

Note

Manage interfaces on page 104 explains how to modify the network interfaces associated with a NAS server.

Format

```
/net/nas/server -id <value> set [-name <value>] [{-enableNFS
{yes | no}] [-enableNFSv4 {yes | no}] [-mpSharingEnabled {yes |
no}] [-unixDirectoryService {ldap | nis | none}] [{-
defaultAccessDisabled | [-defaultUnixUser <value>] [-
defaultWindowsUser <value>]}] [-extendedUnixCredEnabled {no|
yes}] [-credCacheRetention <value>]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the NAS server to change.

Action qualifiers

Qualifier	Description
-name	Specifies the new NAS server name.
-enableNFS	Enables NFSv3 file systems on the NAS server. Valid values are: • yes (default) • no
-enableNFSv4	Specifies whether NFS shares can be accessed using the NFSv4 protocol. Valid values are: • yes • no (default) **Note** NFSv3 file systems are also enabled when the NFSv4 protocol is enabled.
-mpSharingEnabled	Indicates whether multiprotocol sharing mode is enabled. Valid values are: • yes • no
-unixDirectoryService	Directory Service used for querying identity information for Unix (such as UIDs, GIDs, net groups). Valid values are: • nis • ldap • none (default)

Qualifier	Description
-defaultAccessDisabled	Disables file access when no user mapping mechanism is found.
-defaultUnixUser	Default Unix user name that grants file access in the multiprotocol sharing mode. This user name is used when the corresponding Unix/Linux user name is not found by the mapping mechanism.
-defaultWindowsUser	Default Windows user name that grants file access in the multiprotocol sharing mode. This user name is used when the corresponding Windows user name is not found by the mapping mechanism.
-extendedUnixCredEnabled	Specifies whether there are more than 16 Unix groups. Valid values are yes or no.
-credCacheRetention	Specifies the amount of time (in minutes) when the credential cache refreshes or times out. Default value is 15 minutes.

Example

The following command updates NAS server nas_1 with these settings:

- Enable support for NFS file systems.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server -id
nas_1 set -enableNFS yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = nas_1
Operation completed successfully.
```

Delete NAS servers

Delete a NAS server.

Prerequisites

Before you can delete a NAS server, you must first delete all storage resources associated with it.

⚠️ **CAUTION**

Deleting a NAS server removes everything configured on the NAS server, but does not delete the storage resources that use it. You cannot delete a NAS server while it has any associated storage resources. After the storage resources are deleted, the files and folders inside them cannot be restored from snapshots. Back up the data from the storage resources before deleting them from the system.

Format
```
/net/nas/server -id <value> delete
```

Object qualifier

Qualifier	Description
-id	Type the ID of the NAS server to delete.

Example

The following command deletes NAS server nas_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server –id nas_1 delete

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage FTP settings

File Transfer Protocol (FTP) is a client/server protocol that operates over TCP/IP and allows file sharing across heterogeneous systems. Secure File Transfer Protocol (SFTP) protocol provides secure file transfer and manipulation functionality by using SSH.

You can configure a NAS server to share files using the FTP or SFTP protocol. Remote clients can be authenticated using a Unix or Windows user name. You can also have the FTP service to accept anonymous user authentication.

Table 22 FTP and SFTP attributes for a NAS server

Attribute	Description
NAS server	Associated NAS server identifier.
FTP enabled	Indicates whether the FTP protocol is enabled. Valid values are: • yes • no
SFTP enabled	Indicates whether the SFTP protocol is enabled. Valid values are: • yes • no
CIFS users enabled	Indicates whether Windows (CIFS) users can be authenticated by the FTP or SFTP server. Valid values are: • yes (default) • no
Unix users enabled	Indicates whether Unix users can be authenticated by the FTP or SFTP server. Valid values are: • yes (default) • no
Anonymous user enabled	Indicates whether the FTP server supports anonymous user authentication. Valid values are:

Table 22 FTP and SFTP attributes for a NAS server (continued)

Attribute	Description
	• `yes` (default) • `no`
`Home directory limitation enabled`	Indicates whether authenticated FTP or SFTP users are limited to their home directories. Valid values are: • `yes` (default) • `no`
`Default home directory`	Indicates the default home directory for the FTP or SFTP users with no defined or accessible home directory.
`Welcome message`	Indicates the welcome message that appears to FTP or SFTP users before authentication.
`Message of the day`	Indicates the message of the day that appears once the FTP or SFTP users log on.

View FTP settings

View FTP or SFTP server settings for a NAS server.

Format
```
/net/nas/ftp [-server <value>] show
```

Object qualifier

Qualifier	Description
`-server`	Type the name of the NAS server.

Example
The following command displays the FTP server settings for a NAS server:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/ftp show`

```
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection

1:    NAS server                = nas_1
      FTP enabled               = yes
      SFTP enabled              = no
      CIFS users enabled        = yes
      Unix users enabled        = yes
      Anonymous user enabled    = no
      Homedir limitation enabled = no
      Default home directory    = /home/public
```

Change FTP settings

Modify existing FTP or SFTP settings of a NAS server.

Format
```
/net/nas/ftp -server <value> set [-ftpEnabled {yes|no}] [-
sftpEnabled {yes|no}] [-authCifsEnabled {yes|no}] [-
```

```
authUnixEnabled {yes|no}] [-anonymousAuthEnabled {yes|no}] [-
homedirLimitEnabled {yes|no}] [-defaultHomedir <value>] [-
welcome <value>] [-motd <value>]
```

Object qualifier

Qualifier	Description
`-server`	Type the name of the NAS server.

Action qualifier

Qualifier	Description
`-ftpEnabled`	Indicates whether the FTP server is enabled on the NAS server. Valid values are: • `yes` • `no` (default)
`-sftpEnabled`	Indicates whether the SFTP server is enabled on the NAS server. Valid values are: • `yes` • `no` (default)
`-cifsUserEnabled`	Indicates whether Windows (CIFS) users can be authenticated by the FTP or SFTP server. Valid values are: • `yes` (default) • `no`
`-unixUserEnabled`	Indicates whether Unix users can be authenticated by the FTP or SFTP server. Valid values are: • `yes` (default) • `no`
`-anonymousUserEnabled`	Indicates whether the FTP server supports anonymous user authentication. Valid values are: • `yes` (default) • `no`
`-homedirLimitEnabled`	Indicates whether authenticated FTP or SFTP users are limited to their home directories. Valid values are: • `yes` (default) • `no`
`-defaultHomedir`	Type the default home directory for the FTP or SFTP users with no defined or accessible home directory.
`-welcome`	Type the welcome message that appears to FTP or SFTP users before authentication.

Qualifier	Description
-motd	Type the message of the day that appears once the FTP or SFTP users log on.

Example

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/ftp -server nas_1 set -ftpEnabled yes -sftpEnabled no -cifsUserEnabled yes - unixUserEnabled yes -anonymousUserEnabled no -homedirLimitEnabled no - defaultHomedir /home/public -welcome "Welcome to this awesome server"

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage LDAP settings of a NAS server

The Lightweight Directory Access Protocol (LDAP) is an application protocol for querying and modifying directory services running on TCP/IP networks. LDAP provides central management for network authentication and authorization operations by helping to centralize user and group management across the network.

You can configure a NAS server to use LDAP or NIS as a Unix Directory Service to map users, retrieve netgroups, and build a Unix credential. When an initial LDAP configuration is applied, the system checks for the type of LDAP server. It can be an Active Directory schema, IPLANET schema, or an RFC 2307 schema. By default, the RFC 2307 schema is generated. Once the schema is identified, the schema is saved inside a ldap.conf file. You can download this LDAP schema, edit it based on your needs, and upload it back again using the CLI commands mentioned in this section.

The following table lists the attributes for LDAP settings for a NAS server.

Table 23 LDAP settings of a NAS server

Attribute	Description
NAS server	Unique identifier of the associated NAS server. The LDAP client configuration object is identified by the NAS server ID.
IP address	Relevant IP addresses of the associated LDAP servers.
Port	The TCP/IP port used by the NAS server to connect to the LDAP servers. Default value for LDAP is 389 and LDAPS is 689.
Protocol	Type of LDAP protocol. Valid values are: • ldap • ldaps For a secure SSL connection, use ldaps.
Authentication type	Type of authentication for the LDAP server. Valid values are: • anonymous • kerberos • simple

Table 23 LDAP settings of a NAS server (continued)

Attribute	Description
`Verify certificate`	Indicates whether Certification Authority certificate is used to verify the LDAP server certificate for secure SSL connections. Valid values are: • `yes` • `no` Value shows as empty when the LDAP protocol is selected (no SSL).Value defaults to yes when the LDAPS protocol is used.
`Use CIFS account` (applies to Kerberos authentication)	Indicates whether CIFS authentication is used. Valid values are: • `yes` – Indicates that the CIFS settings are used for Kerberos authentication. • `no` – Indicates that Kerberos uses its own settings.
`Principal` (applies to Kerberos authentication)	Specifies the principal name for Kerberos authentication.
`Realm` (applies to Kerberos authentication)	Specifies the realm name for Kerberos authentication.
`Password` (applies to Kerberos authentication)	Specifies the associated password for Kerberos authentication.
`Bind DN` (applies to Simple authentication)	Specifies the Distinguished Name (DN) used when binding.
`Bind password` (applies to Simple authentication)	Specifies the associated password used when binding.
`Base DN`	Specifies the DN of the root level in the directory tree.
`Profile DN`	For an iPlanet LDAP server, specifies the DN of the entry with the configuration profile.

View LDAP settings of a NAS server

View LDAP settings of a NAS server.

Format
`/net/nas/ldap [-server <value>] show`

Object qualifier

Qualifier	Description
`-server`	Name of the associated NAS server.

Example
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/ldap -server nas_1 show -detail

```
1: NAS server      = nas_1
```

```
IP address      = 10.64.74.64, 10.64.74.74
Port            = 636
Protocol        = ldaps
Authentication  = simple
Use CIFS account =
Principal       =
Realm           =
Bind DN         = cn=administrator,cn=User,dc=emc,dc=com
Base DN         = dc=mec,dc=com
Profile DN      =
```

Change LDAP settings of a NAS server

Modify LDAP settings of a NAS server.

Format

```
/net/nas/ldap -server <value> set {-enabled no | [ -ip <value>]
[-port <value>] [-protocol {ldap | ldaps}] [-verifyCert {yes |
no}] [-authType {anonymous | kerberos {-useCifsAccount | -
principal <value> [-realm <value>] [{-password <value> | -
passwordSecure }]} | simple [-bindDn <value> {-bindPasswd
<value> | -bindPasswdSecure}]}] [-baseDn <value>] [-profileDn
<value>]}
```

Object qualifier

Qualifier	Description
-server	Identifies the associated NAS server.

Action qualifier

Qualifier	Description
-enabled	Indicates whether the LDAP settings is enabled for the NAS server. Valid values is no. **Note** Setting the value to no removes the LDAP settings for an existing NAS server.
-ip	Type the IP addresses (separated by comma) of the associated LDAP servers.
-port	Type the port associated with the LDAP server.
-protocol	Type the protocol to be used. Valid values are: • ldap • ldaps For a secure SSL connection, use ldaps.
-verifyCert	Specify that uploaded Certification Authority (CA) certificates should be used to verify the certificates of LDAP servers for establishing secure SSL connections. Valid values are: • yes • no

Qualifier	Description
	Applicable only when the protocol is LDAPS. Value shows as empty when LDAP (no SSL) is used.
-authType	Specify the type of authentication for the LDAP server. Valid values are: • `anonymous` • `kerberos` • `simple`
-bindDn	Type the Distinguished Name (DN) to be used when binding to the server.
-bindPasswd	Type the associated password to be used when binding to the server.
-bindPasswdSecure	Type the password in secured mode. You will be prompted to enter the password separately.
-useCifsAccount	Specify whether you want to use CIFS authentication. For Kerberos authentication only.
-principal	Type the principal name for Kerberos authentication.
-realm	Type the realm name for Kerberos authentication.
-password	Type the associated password for Kerberos authentication.
-baseDn	Type the DN of the root level in the directory tree.
-profileDn	For an iPlanet LDAP server, type the DN of the entry with the configuration profile.

Example

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/ldap -
server nas_1 set -ip 10.64.74.64,10.64.74.74 -port 636 -authType
simple -protocol ldaps -bindDn
"cn=administrator,cn=User,dc=emc,dc=com" -bindPasswd "Ldap123!" -
baseDn "dc=mec,dc=com"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Upload an LDAP schema

You can customize the LDAP schema for your NAS server, and upload the new schema file. Once the schema is uploaded, it gets validated. If the schema is valid, it is applied, and your NAS server LDAP configuration is changed.

Example

```
uemcli -upload -f "LDAP_nas_1.conf" -d 10.0.0.1 -u Local/joe -p
MyPassword456! /net/nas/ldap -server nas_1 -type config
```

```
Storage system address: 10.0.0.1
Storage system port: 443
```

```
HTTPS connection

Operation completed successfully.
```

Download an LDAP schema

When an initial LDAP configuration is applied, the system checks for the type of LDAP server. Once the schema is identified, the schema is saved inside a ldap.conf file. You can download this LDAP schema using the -download switch, and customize it based on your needs. For more information on switches, see Switches on page 14

Example

uemcli -download -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/ ldap -server nas_1 -type config

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Upload a Certification Authority certificate

You can upload Certification Authority (CA) certificates for your NAS LDAP servers. Once you upload the CA certificate, it can be used for validating certificates of an LDAP server.

Example

uemcli –upload -f "MyCert.pem" -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/ldap –server nas_1 –type CACertificate

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Download a Certification Authority certificate

A Certification Authority (CA) certificate is used for validating certificates of an LDAP server.

Example

uemcli –download -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/ ldap –server nas_1 –type CACertificate

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage CIFS Servers

CIFS servers use the CIFS protocol to transfer files. A CIFS server can participate as a member of a Windows Active Directory domain or operate independently of any Windows domain as a standalone CIFS server.

The following table lists the attributes for CIFS servers.

Table 24 CIFS Server attributes

Attribute	Description
ID	ID of the CIFS server.
NAS server	Associated NAS server ID.
Name	Name of the CIFS server.
NetBIOS name	Server NetBIOS name.
Windows domain	Windows server domain name.
User name	Windows domain user name.
Password	Windows domain user password.
Organization unit	For support of CIFS file systems, the organizational unit setting for the Active Directory domain. In Active Directory, organizational units represent containers where users, groups, computers, and other organizational units are organized. They provide the smallest scope or unit to which you can assign Group Policy settings or delegate administrative authority in an Active Directory environment. **Note** The Unisphere online help provides more details about this attribute.
Workgroup	Workgroup name.
Workgroup administrator password	Workgroup administrator password.

Create CIFS server

Create a CIFS server.

Note

Only one CIFS server per file server can be created.

Format
```
/net/nas/cifs create -server <value> [-name <value>] [-
netbiosName <value>] {-domain <value> -username <value> {-
passwd <value> | -passwdSecure <value>} {-orgUnit <value>]} | -
workgroup <value> {-adminPasswd <value> | -adminPasswdSecure} }
```

Action qualifiers

Qualifier	Description
-server	Specifies the NAS server identifier.
-name	Specifies the CIFS server name. The default value is the name of the NAS server.

Qualifier	Description
-netbiosName	Specifies the CIFS server NetBIOS name. By default it is generated automatically based on the CIFS server name.
-domain	Specifies Windows server domain name.
-username	Specifies the domain user.
-passwd	Specifies the domain user password.
-passwdSecure	Specifies the password in secure mode - the user will be prompted to input the password and the password confirmation.
-orgUnit	Active directory organizational unit.
-workgroup	Specifies the workgroup of the standalone CIFS server.
-adminPasswd	Specifies the new local admin password of the standalone CIFS server.
-adminPasswdSecure	Specifies the password in secure mode. You will be prompted to enter the password and the password confirmation.

Example

The following command creates a CIFS server.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/cifs create -server FS_0 -name CIFSserver1 -domain domain.one.com -username user1 -passwd password1

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = CIFS_0
Operation completed successfully.
```

View CIFS server

The following command displays CIFS server settings.

Format

/net/nas/cifs [{-id <*value*> | -server <*value*>}] show

Object qualifier

Qualifier	Description
-id	Identifies the CIFS server.
-server	Identifies the associated NAS server.

Example

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/cifs show

```
Storage system address: 10.0.0.1
Storage system port: 443
```

```
HTTPS connection

1:      ID            = CIFS_0
        File server   = FS_0
        Name          = CIFSserver1
        NetBIOS name  = CIFSserv
        Windows domain = domain.one.com
```

Change CIFS server settings

Modify an existing CIFS server.

Format
```
/net/nas/cifs -id <value> set [-name <value>] [-netbiosName
<value>] [-currentUsername <value> {-currentPasswd <value> | -
currentPasswdSecure} ] { [-domain <value>] [-newUsername
<value> {-newPasswd <value> | -newPasswdSecure} ] | [-workgroup
<value>] [ {-adminPasswd <value> | -adminPasswdSecure} ] }
```

Object qualifier

Qualifier	Description
-id	Type the ID of the CIFS server to change.

Action qualifiers

Qualifier	Description
-name	Specifies the new CIFS server name.
-netbiosName	Specifies the new CIFS server NetBIOS name.
-domain	Specifies the new Windows server domain name.
-currentUsername	Specifies the current domain user.
-currentPasswd	Specifies the current domain user password.
-currentPasswdSecure	Specifies the current password in secure mode - the user will be prompted to input the password and the password confirmation.
-newUsername	Specifies the new domain user.
-newPasswd	Specifies the new domain user password.
-newPasswdSecure	Specifies the new password in secure mode - the user will be prompted to input the password and the password confirmation.
-workgroup	Specifies the new workgroup of the standalone CIFS server.
-adminPasswd	Specifies the new local admin password of the standalone CIFS server.
-adminPasswdSecure	Specifies the password in secure mode - the user will be prompted to input the password and the password confirmation.

Example

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/cifs -id
CIFS_0 set -workgroup MyWorkgroup -adminPasswd MyPassword
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = CIFS_0
Operation completed successfully.
```

Delete CIFS server

Delete an existing CIFS server.

Note

When you delete an existing CIFS server or convert it to a standalone configuration, you must specify its username and password to unjoin it. If you ran this command without the username and password, you will not be able to join the CIFS server with the same name back again. To join the same CIFS server back to the domain, you will then need to first change its name.

Format

```
/net/nas/cifs -id <value> delete [ {-username <value> {-passwd
<value> | -passwdSecure} | -skipUnjoin} ]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the CIFS server to delete.

Action qualifiers

Qualifier	Description
-username	Specifies the domain user. Not required for standalone CIFS servers. **Note** To unjoin the CIFS server from a domain, specify the username.
-passwd	Specifies the domain user password. Not required for standalone CIFS servers. **Note** To unjoin the CIFS server from a domain, specify the password.
-passwdSecure	Specifies the password in secure mode - the user will be prompted to input the password and the password confirmation.
-skipUnjoin	Delete the CIFS server without unjoining it from the domain.

Example

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/cifs -id
CIFS_0 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = CIFS_0
Operation completed successfully.
```

Manage reverse CHAP for mutual CHAP authentication

The Challenge Handshake Authentication Protocol (CHAP) is a security protocol that defines a method for authenticating hosts (initiators) and iSCSI nodes (targets). When CHAP is enabled, an iSCSI target will "challenge" an initiator that attempts to establish a connection with it. If the initiator does not respond with a valid password (called a secret), the target refuses the connection. CHAP authentication can be one-way, where only the target authenticates the initiator, or reverse (also called mutual), where the target and initiator authenticate each other. Compared to one-way CHAP, enabling reverse CHAP provides an extra level of security. To set one-way CHAP authentication, create an iSCSI CHAP account for a host. Manage iSCSI CHAP accounts for one-way CHAP authentication on page 154 explains the commands for configuring one-way CHAP authentication.

Note

For reverse CHAP, the secret password you specify applies to all iSCSI nodes on the system. Also, the CHAP secret specified for any host configuration must be different from the reverse CHAP password specified for iSCSI nodes.

The iSCSI reverse CHAP object manages the username/secret used by the target (storage system) to respond to a challenge from an initiator (host).

Specify reverse CHAP secret settings

The following table lists the iSCSI reverse CHAP attributes.

Table 25 iSCSI reverse CHAP attributes

Attribute	Description
Username	The reverse CHAP user name.
Secret	The reverse CHAP secret (password).
Secret format	The reverse CHAP input format. Value is one of the following: • ASCII -- ASCII format • Hex -- Hexadecimal format

Sets the reverse CHAP username and secret.

Format
```
/net/iscsi/reversechap set { [-username <value>] {-secret
<value> | -secretSecure} [-secretFormat { ascii | hex } ] | -
noChap}
```

Action qualifiers

Qualifier	Description
-username	The reverse CHAP user name.
-secret	Specifies the reverse CHAP secret (password). **Note** Restrictions: the CHAP secret is an ASCII string that is 12 to 16 characters. Hexadecimal secrets are 12 to 16 pairs of data (24 to 32 characters).
-secretSecure	Specifies the password in secure mode - the user will be prompted to input the password.
-secretFormat	The reverse CHAP input format. Value is one of the following: • ASCII -- ASCII format • Hex -- Hexadecimal format
-noChap	Remove the reverse CHAP credentials.

Example

uemcli /net/iscsi/reversechap set -secret xyz0123456789

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

View reverse CHAP secret settings

View whether a reverse CHAP secret password has been configured for iSCSI nodes.

Note

explains how to change the output format.

Format
/net/iscsi/reversechap show

Example
The following command shows the current reverse CHAP setting:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/iscsi/
reversechap show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      Username = ReverseChapUser
```

Set up iSNS for iSCSI storage

The iSNS protocol (iSNSP) allows centralized management of iSCSI devices. An iSNS server can provide services such as remote discovery and configuration for iSCSI nodes

and hosts. When iSNSP is in use, both the iSCSI nodes (targets) and hosts (initiators) on the network must be configured to use the iSNS server. You create a single iSNS server record for the system. The following table lists the attributes for iSNS server records.

Table 26 iSNS server record attributes

Attribute	Description
ID	ID of the iSNS server record.
Server	Name or IP address of an iSNS server.

Create iSNS server records

Create an iSNS server record to specify an iSNS server for the system to use. When you create an iSNS server record, it will overwrite the existing record on the system.

Format
`/net/iscsi/isns create -server <value>`

Action qualifiers

Qualifier	Description
-server	Type the name or IP address of the iSNS server.

Example
The following command creates an iSNS server record for server IP address 10.5.2.128. The server record receives the ID iSNS_10.5.2.128:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/iscsi/isns

create -server 10.5.2.128

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = isns_0
Operation completed successfully.
```

View iSNS server records

View details for configured iSNS server records.

Note

explains how to change the output format.

Format
`/net/iscsi/isns show`

Example
The following command shows details for the iSNS server record:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/iscsi/isns show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = isns_0
Operation completed successfully.
```

Delete iSNS server records

Delete an iSNS server record.

Format
```
/net/iscsi/isns -id <value> delete
```

Object qualifier

Qualifier	Description
-id	Type the ID of the iSNS server record to delete.

Example
The following command deletes the iSNS server record isns_0:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/iscsi/isns -id isns_0 delete

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Change iSNS server record settings

Modify an existing iSNS server record.

Format
```
/net/iscsi/isns -id <value> set -server <value>
```

Object qualifier

Qualifier	Description
-id	Type the ID of the iSNS server record to delete.

Action qualifiers

Qualifier	Description
-server	New IP address associated with the iSNS server.

Example
The following command modifies the iSNS server record:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/iscsi/isns -id isns_0 set -server 10.5.2.130

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = isns_0
Operation completed successfully.
```

Manage iSCSI configuration

The following table lists the attributes for iSCSI configuration.

Table 27 ISCSI configuration attributes

Attribute	Description
`CHAP required`	Specifies whether CHAP authentication is required in order to access iSCSI storage. Valid values are: • `yes` • `no`

View iSCSI configuration

View details about the iSCSI configuration.

Format
```
/net/iscsi/config show
```

Example
The following command shows details for the iSCSI configuration:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/iscsi/config show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: CHAP required = yes
```

Change iSCSI configuration

Modify the iSCSI configuration.

Format
```
/net/iscsi/config set -chapRequired {yes | no}
```

Object qualifier

Qualifier	Description
`-chapRequired`	Specify whether CHAP authentication is required. Values are case-sensitive. Valid values are: • `yes` • `no`

Example
The following command denies host access without CHAP authentication:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/iscsi/config
set -chapRequired yes
```

```
Storage system address:10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage iSCSI nodes (servers)

iSCSI nodes, or iSCSI Servers, are software components on the system that are dedicated to managing operations for data transferred through the iSCSI protocol. iSCSI nodes run on each Ethernet port and communicate with network hosts through the SP ports.

iSCSI nodes handle storage creation, monitoring, and management tasks for iSCSI LUNs. Hosts connect to the LUN through iSCSI initiators.

Each iSCSI node is identified by an ID.

Manage reverse CHAP for mutual CHAP authentication on page 89 explains how to configure reverse CHAP authentication between iSCSI hosts and nodes.

The following table lists the attributes for iSCSI nodes.

Table 28 iSCSI node attributes

Attribute	Description
ID	ID of the iSCSI node.
Alias	Name of the iSCSI node.
IQN	iSCSI qualified name (IQN) for the node. The iSCSI protocol outlines a specific address syntax for iSCSI devices that communicate on a network. The iSCSI addresses are called IQNs. Each IQN includes a Type field, Date field, Naming Authority field, and String field. For example: `iqn.` `1992-07.com.emc:apm000650039080000-3`
SP	Primary SP on which the node runs..
Health state	Health state of the iSCSI node. The health state code appears in parentheses. Value is one of the following: • `Unknown (0)` — Status is unknown. • `OK (5)` — Working correctly. • `Degraded/Warning (10)` — Working and performing all functions, but the performance may not be optimum. • `Critical failure (25)` — Failed and recovery may not be possible. This condition has resulted in data loss and should be remedied immediately.
Health details	Additional health information. See Appendix A, Reference, for health information details.
Port	Associated network port identifier.
Interfaces	ID of each network interface assigned to the iSCSI node. The interface defines the IP address for the node and allows it to communicate with the network and hosts.

Table 28 iSCSI node attributes (continued)

Attribute	Description
	Note Manage interfaces on page 104 explains how to configure network interfaces on the system.

View iSCSI nodes

View details about iSCSI nodes. You can filter on the iSCSI node ID.

Note

The show action command on page 17 explains how to change the output format.

Format
```
/net/iscsi/node [-id <value>] show
```

Object qualifier

Qualifier	Description
-id	Type the ID of an iSCSI node.

Example
The following command lists all iSCSI nodes on the system:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/iscsi/node show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:     ID          = ISCSIN_1
       Alias       = MyISCSIserver1
       IQN         = iqn.
1992-05.com.emc:fcnch0821001340000-1
       Health state = OK (5)
       SP          = SPA
       Port        = eth0_SPA
       Interfaces  = IF_1,IF_2

2:     ID          = ISCSIN_2
       Name        = MyISCSIserver2
       IQN         = iqn.
1992-05.com.emc:fcnch0821001340001-1
       Health state = OK (5)
       SP          = SPA
       Port        = eth1_SPA
       Interfaces  = IF_3
```

Change iSCSI node settings

Change the network interface alias assigned to the node.

Format
```
/net/iscsi/node -id <value> set -alias <value>
```

Object qualifier

Qualifier	Description
-id	Type the ID of the iSCSI node to change.

Action qualifier

Qualifier	Description
-alias	User-friendly name that identifies the iSCSI node.

Example

The following command assigns an alias to the ISCSIN_1 node:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/iscsi/node -id ISCSIN_1 set -alias "My iSCSI node"

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = ISCSIN_1
Operation completed successfully.
```

Manage Ethernet ports

View and change the settings for the network ports on each SP.

The following table describes the port attributes.

Table 29 Network port attributes

Attribute	Description
ID	ID of the port.
Name	Name of the port.
SP	Name of the SP on which the port resides. Value is SPA or SPB.
Protocol	Types of protocols the port supports. Value is one of the following: • mgmt — Management interface. • file — Network interface for Windows (CIFS) and Linux/UNIX (NFS) storage. • iscsi — iSCSI interface for iSCSI storage. Manage interfaces on page 104 explains how to configure network interfaces on the system.
MTU size	Maximum transmission unit (MTU) packet size (in bytes) that the port can transmit. Default is 1500 bytes per packet.
Requested MTU size	MTU size set by the user.
Available MTU size	List of available MTU sizes.

Table 29 Network port attributes (continued)

Attribute	Description
Speed	Current link speed of the port.
Requested speed	Link speed set by the user.
Available speeds	List of available speed values.
Health state	Health state of the port. The health state code appears in parentheses. Value is one of the following: • Unknown (0) — Status is unknown. • OK (5) — Port is operating normally. • OK BUT (7) — Lost communication, but the port is not in use. • Minor failure (15) — Lost communication. Check the network connection and connected cables. • Major failure (20) — Port has failed. Replace the SP that contains the port.
Health details	Additional health information. See Appendix A, Reference, for health information details.
Aggregated port ID	If the port is in a link aggregation, the ID of the link aggregation appears. Manage link aggregations on page 113 explains how to configure link aggregations on the SP ports.
Connector type	Physical connector type. Valid values are: • unknown • RJ45 • LC • MiniSAS_HD

View Ethernet port settings

View details about the network ports. You can filter on the port ID.

Note

The show action command on page 17 explains how to change the output format.

Format
```
/net/port/eth [-id <value>] show
```

Object qualifier

Qualifier	Description
-id	Type the ID of the port.

Example

`uemcli /net/port/eth show`

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID                = spa_mgmt
        Name              = mgmt
        SP                = spa
        Protocols         = mgmt
        MTU size          = 1500
        Speed             = 100 Mbps
        Health state      = OK (5)
        Aggregated port ID =

2:      ID                = spa_eth0
        Name              = eth0
        SP                = spa
        Protocols         = file, iscsi
        MTU size          = 1500
        Speed             = 10 Gbps
        Health state      = OK (5)
        Aggregated port ID = la0_SPA

3:      ID                = spa_eth1
        Name              = eth1
        SP                = spa
        Protocols         = file, iscsi
        MTU size          = 9000
        Speed             = 1 Gbps
        Health state      = OK (5)
        Aggregated port ID = la0_SPA

4:      ID                = spa_iom_0_eth0
        Name              = eth2
        SP                = spa
        Protocols         = file, iscsi
        MTU Size          = 9000
        Speed             = 1 Gbps
        Health state      = OK (5)
        Aggregated port ID = None
```

Change Ethernet port settings

Note

The new settings are applied to a pair of symmetrical ports on dual SP systems.

Change the maximum transmission unit size and port speed for an Ethernet port.

Format
`/net/port/eth -id <value> set [-mtuSize <value>] [-speed <value>]`

Object qualifier

Qualifier	Description
-id	Type the ID of the network port.

Action qualifier

Qualifier	Description
-mtuSize	Type the maximum transmission unit packet size (in bytes) for the port.
-speed	Type the port speed.

Example

The following command sets the MTU size for Ethernet port 0 (eth0) on SP A to 9000 bytes:

uemcli /net/port/eth -id spa_eth0 set -mtuSize 9000

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = spa_eth0
ID = spb_eth0
Operation completed successfully.
```

Manage SAS ports (physical deployments only)

View the settings for the SAS ports on each SP. The following table describes the port attributes.

Table 30 SAS port attributes

Attribute	Description
ID	ID of the port.
Name	Name of the port.
SP	Name of the SP on which the port resides. Value is SPA or SPB.
Speed	Current link speed of the port.
Health state	Health state of the port. The health state code appears in parentheses. Value is one of the following: • Unknown (0) — Status is unknown. • OK (5) — Port is operating normally. • OK BUT (7) — Lost communication, but the port is not in use. • Minor failure (15) — Lost communication. Check the network connection and connected cables. • Major failure (20) — Port has failed. Replace the SP that contains the port.
Health details	Additional health information. See Appendix A, Reference, on page 367 for health information details.
Connector type	Physical connector type. Valid values are: • unknown • RJ45 • LC

Table 30 SAS port attributes (continued)

Attribute	Description
	● `MiniSAS_HD`

View SAS settings

View details about the SAS ports. You can filter on the port ID.

Note

explains how to change the output format.

Format
```
/net/port/sas [-id <value>] show
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the port.

Example
`uemcli /net/port/sas show`

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:     ID           = spa_sas0
       Name         = SP A SAS Port 0
       SP           = spa
       Speed        =
       Health state = OK_BUT (7)

2:     ID           = spa_sas1
       Name         = SP A SAS Port 1
       SP           = spa
       Speed        = 6 Gbps
       Health state = OK (5)
```

Manage FC ports

View and change the settings for the FC ports on each SP.

The following table describes the port attributes.

Table 31 FC port attributes

Attribute	Description
`ID`	ID of the port.
`Name`	Name of the port.
`SP`	Name of the SP on which the port resides.

Table 31 FC port attributes (continued)

Attribute	Description
WWN	World Wide Name (WWN) of the port.
Speed	Current link speed of the port.
Requested speed	Link speed set by the user.
Available speed	List of available speed values.
Health state	Health state of the port. The health state code appears in parentheses. Value is one of the following: • Unknown (0) — Status is unknown. • OK (5) — Port is operating normally. • OK BUT (7) — Lost communication, but the port is not in use. • Minor failure (15) — Lost communication. Check the network connection and connected cables. • Major failure (20) — Port has failed. Replace the SP that contains the port.
Health details	Additional health information. See Appendix A, Reference, for health information details.
Connector type	Physical connector type. Valid values are: • unknown • RJ45 • LC • MiniSAS_HD

View FC port settings

View details about the FC ports. You can filter on the port ID.

Note

explains how to change the output format.

Format
/net/port/fc [-id <*value*>] show

Object qualifier

Qualifier	Description
-id	Type the ID of the port.

Example

```
uemcli /net/port/fc show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID                 = spa_fc1
        Name               = fc1
        SP                 = spa
        WWN                = 50:06:BD:01:60:05:8E:
50:06:01:64:3D:E0:05:8E
        Speed              = 1 Gbps
        Requested speed    = auto
        Available speeds   = auto, 1 Gbps, 2 Gbps, 4 Gbps
        Health state       = OK (5)
        Health details     = "The port is operating normally."
```

Change port settings

Change the speed for an FC port.

Format

```
/net/port/fc -id <value> set -speed <value>
```

Object qualifier

Qualifier	Description
–id	Type the ID of the FC port.

Action qualifier

Qualifier	Description
–speed	Type the port speed.

Example
The following command sets the speed for FC port fc1 on SP A to 1 Gbps:

```
uemcli /net/port/fc –id spa_fc1 set –speed 1Gbps
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = spa_fc1
Operation completed successfully.
```

Management network interfaces

Configure management network interfaces to remotely manage and monitor the system, the network, and configured hosts. Specify the IP address for the interface as well as the IP addresses for the subnet mask and gateway. View details about existing management interfaces configured on the system through the Connection Utility. Each management interface is identified by its IP protocol version. IPv4 and IPv6 can be configured, independently of each other, at the same time, but they cannot both be disabled at the same time. The netmask can be specified with the appropriate prefix length, separated from the IP address with a /, such as 10.0.0.1/24. This is optional for IPv4, but required

for IPv6. There can be up to five IPv6 addresses assigned automatically. Only one IPv6 address can be set manually.

The following table lists the interface attributes with a description of each.

Table 32 Interface attributes

Attribute	Description
IP protocol version	IP protocol version. Value is one of the following: • `ipv4` • `ipv6`
Address origin	IP settings origin. Value is one of the following: • `Disabled`— Indicates the interface is disabled. • `Automatic`— Indicates the IP attributes are set automatically by DHCP or SLAAC (IPv6 only). • `Static`— Indicates the IP attributes are set manually.
IP address	IPv4 or IPv6 address.
Subnet mask	IPv4 subnet mask.
Gateway	IPv4 or IPv6 gateway.
MAC address	MAC address associated with the interface.

View management interfaces

View a list of interfaces on the system. You can filter on the interface ID.

Format
`/net/if/mgmt show`

Example
The following command displays all management interfaces on the system:

uemcli /net/if/mgmt show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      IP protocol version = ipv4
        Address origin      = static
        IP address          = 10.0.0.1
        Subnet mask         = 255.255.255.0
        Gateway             = 10.0.0.2

2:      IP protocol version = ipv6
        Address origin      = automatic
        IP address          = 3ffe:80c0:22c:4e:a:0:2:7f/64
        Subnet mask         =
        Gateway             = 3ffe
```

Change interface settings

Change the settings for an interface.

Format

```
/net/if/mgmt set { -ipv4 | -ipv6 } {disabled | automatic |
static [-addr <value>] [-netmask <value>] [-gateway <value>] }
```

Action qualifier

Qualifier	Description
-ipv4	Specifies the IPv4 origin. Value is one of the following: • `Disabled`— Indicates the interface is disabled. • `Automatic` — Indicates the IP attributes are set automatically by DHCP. • `Static` — Indicates the IP attributes are set manually
-ipv6	Specifies the IPv6 origin. Value is one of the following: • `Disabled` — Indicates the interface is disabled. • `Automatic` — Indicates the IP attributes are set automatically by DHCP. or SLAAC.Multiple addresses are possible • `Static` — Indicates the IP attributes are set manually.
-addr	Specifies the IPv4 or IPv6 address of the interface. Optionally, you can also specify the prefix length in the following format: `<IP address>/` `<prefix length>`. **Note** The default prefix length for IPv6 is 64.
-netmask	Specifies the IPv4 subnet mask for the interface. **Note** This is optional if you specify the prefix length in the `-addr` attribute.
-gateway	Specifies the IPv4 or IPv6 gateway for the interface.

Example

The following command changes the IP address, the netmask, and the gateway for interface IF_1:

uemcli /net/if/mgmt set -ipv4 static -addr 192.168.1.1 -netmask
255.255.255.0 -gateway 192.168.1.2

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage interfaces

Create interfaces to enable and control access between the system, the network, and configured hosts. Specify the IP address for the interface as well as the IP addresses for the subnet mask and gateway.

You can create the following types of interfaces:

- iSCSI interfaces for controlling access to iSCSI storage. You assign the interface to an iSCSI node.
- Replication interfaces for replication-related data or management traffic.

Each interface is identified by an ID.

The following table lists the interface attributes with a description of each.

Table 33 Interface attributes

Attribute	Description
ID	ID of the interface.
Type	Interface type. Value is one of the following: • `file` — Interface for CIFS or NFS storage. • `iscsi`— Interface for iSCSI storage. • `replication` — Interface for replication-related data or management traffic.
Port	ID of the physical port or link aggregation on an SP on which the interface is running. The ID includes the port name and SP name.
VLAN ID	Virtual local area network (VLAN) ID for the interface. The interface uses the ID to accept packets that have VLAN tags. The value range is 1-4095. **Note** If no VLAN ID is specified, which is the default, packets do not have VLAN tags. The Unisphere online help provides more details about VLANs.
IP address	IPv4 or IPv6 address.
Subnet mask	IPv4 subnet mask.
Gateway	IPv4 or IPv6 gateway.
MAC address	MAC address of the interface.
SP	SP that uses the interface.
NAS server	NAS server identifier.
Preferred	Sets the network interface as the preferred source for outgoing traffic. All outgoing DNS or Active Directory requests are forwarded through this interface, and the IP address assigned to this interface is used as the source address of the data packets. For each NAS server, you can choose a single IP address as preferred. Valid values are yes or no. **Note** This attribute applies to file interfaces only.
Health state	A numerical value indicating the health of the system. Value is one of the following: • `Unknown (0)` • `OK (5)`

Table 33 Interface attributes (continued)

Attribute	Description
	• OK BUT (7) • Degraded/Warning (10) • Minor failure (15) • Major failure (20)
Health details	Additional health information.

Create interfaces

Create an interface.

Format

```
/net/if create [-vlanId <value>] -type { {file} -server <value>
| iscsi} -port <value> | mgmt | replication} -origin {dynamic |
static -addr <value>] [-netmask <value>] [-gateway <value>]
```

Action qualifier

Qualifier	Description
-type	Type the interface type. Value is one of the following: • file — Interface for file-based storage, such as file systems. • iscsi — Interface for iSCSI storage. • replication — Interface for replication-related data or management traffic.
-server	Type the NAS server identifier. **Note** A NAS server cannot have more than one IPv4 interface and one IPv6 interface.
-preferred	Specify this qualifier to set the network interface as the preferred source for outgoing traffic. For each NAS server, you can choose an IPv4 interface and IPv6 interface as the preferred interfaces.
-port	Type the ID of the SP port or link aggregation that will use the interface. Manage Ethernet ports on page 96 explains how to view the port IDs. **Note** For systems with two SPs, a file interface is created on a pair of symmetric Ethernet ports rather than on a single specified port. Its current port is defined by NAS server SP and may differ from the specified port. For example, if the user specifies port spa_eth2, but the NAS server is on SP B, the interface is created on port spb_eth2.

Qualifier	Description
-vlanId	Type the virtual LAN (VLAN) ID for the interface. The interface uses the ID to accept packets that have VLAN tags. The value range is 1–4095. **Note** If no VLAN ID is specified, which is the default, packets do not have VLAN tags. The Unisphere online help provides more details about VLANs.
-addr	Type the IP address for the interface. The prefix length should be appended to the IPv6 address and, if omitted, will default to 64. For IPv4 addresses, the default length is 24. The IPv4 netmask may be specified in address attribute after slash.
-netmask	Type the subnet mask for the interface. **Note** This qualifier is not required if the prefix length is specified in the -addr attribute.
-gateway	Type the gateway for the interface. **Note** This qualifier configures the default gateway for the specified port's SP.

Example 1

The following command creates a replication interface. The interface receives the ID IF_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/if create -type replication -port eth1_spb -addr 10.0.0.1 -netmask 255.255.255.0 -gateway 10.0.0.1

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = IF_1
Operation completed successfully.
```

Example 2

The following command creates a network interface for file storage on SP A port eth0 with an IPv6 IP address. The interface receives the ID IF_2:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/if create -type file -server nas_1 -port eth0_SPA -addr 2001:db8:4c: 8130:260:1600:3ed0:a3fe/64

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = IF_2
Operation completed successfully.
```

View interfaces

View a list of interfaces on the system. You can filter on the interface ID.

Note

explains how to change the output format.

Format

```
/net/if [ {-id <value> | -port <value> | -server <value> | -
type <value>} ] show
```

Object qualifier

Qualifier	Description
-id	Type the ID of an interface.
-port	Type the port the interface is associated with.
-server	Type the NAS server the interface is associated with.
-type	Specify the type of the interface. Value is one of the following: • file • iscsi • replication

Example

The following command displays all interfaces on the system:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/if show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID                      = if_0
        Type                    = file
        NAS server              = nas_0
        Preferred               = yes
        Port                    = eth0_spa
        VLAN ID                 = 0
        IP address              = 3ffe:80c0:22c:4e:a:0:2:7f/64
        Subnet mask             =
        Gateway                 = fe80::20a8bff:fe5a:967c
        SP                      = SPA

2:      ID                      = if_1
        Type                    = file
        NAS server              = nas_1
        Preferred               = yes
        Port                    = eth1_spa
        VLAN ID                 = 1
        IP address              = 192.168.1.2
        Subnet mask             = 255.255.255.0
        Gateway                 = 192.168.1.254
        SP                      = SPA

3:      ID                      = if_2
        Type                    = replication
        NAS server              =
```

```
        Preferred               = no
        Port                    = eth1_spb
        VLAN ID                 =
        IP address              = 10.103.75.56
        Subnet mask             = 255.255.248.0
        Gateway                 = 10.103.72.1
        SP                      = spb
```

Change interface settings

Change the settings for an interface.

Format
```
/net/if -id <value> set [-vlanId <value>] [-addr <value>] [-
netmask <value>] [-gateway <value>][-preferred]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the interface to change.

Action qualifier

Qualifier	Description
-vlanId	Type the virtual LAN (VLAN) ID for the interface. The interface uses the ID to accept packets that have VLAN tags. The value range is 1–4095. **Note** If no VLAN ID is specified, which is the default, packets do not have VLAN tags. The Unisphere online help provides more details on VLANs.
-addr	Specify the IP address for the interface. **Note** The prefix length should be appended to the IPv6 address. The IPv4 netmask may be specified in address attribute after the slash.
-netmask	Specify the IPv4 subnet mask for the interface.
-gateway	Specify the gateway for the interface. **Note** The gateway is optional for both IPv4 and IPv6. This qualifier configures the default gateway for the specified port's SP.
-preferred	Specify this qualifier to set the network interface as the preferred source for outgoing traffic. For each NAS server, you can choose an IPv4 interface and IPv6 interface as the preferred interfaces. **Note** This attribute applies to file interfaces only.

Example

The following command changes the gateway address for interface IF_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456!/net/if -id IF_1 set
-gateway 2001:db8:0:170:a:0:2:70

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = IF_1
Operation completed successfully.
```

Delete interfaces

Delete an interface.

> ⚠ **CAUTION**

Deleting an interface can break the connection between systems that use it, such as configured hosts.

Format
/net/if -id <*value*> delete

Object qualifier

Qualifier	Description
-id	Type the ID of the interface to delete.

Example

The following command deletes interface IF_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/if -id IF_1
delete

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage static IP routes

A route determines where to forward a packet next so it can reach its destination, whether that destination is a network or host. A static route is a hard-coded path in the router that specifies how the router will get to a certain subnet by using a certain path. All routes have a value that allows the router to assign a priority to which type of routing is used first. In static routes, the value is 1 which means no matter what other protocol is running, the static route is used first.

Note

An IP route connects an interface (IP address) to the larger network through a gateway. Without the route, the interface is no longer accessible outside its immediate subnet. As a result, network shares and exports associated with the interface are no longer available to clients outside of its immediate subnet.

Each route is identified by an ID.

The following table describes the attributes for static IP routes.

Table 34 Static IP route attributes

Attribute	Description
ID	ID of the route.
Interface ID	ID of the interface the route uses to reach the gateway. The interface is associated with a SP. View interfaces on page 108 explains how to view the network interface IDs.
Route type	Type of route. Values are: • default — Default gateway the system uses when it cannot find a route to a connected node. • host — Static route to a specific host. • net — Static route to a subnet IP address.
Target	IP address of the target network node based on the specified route type. Value is one of the following: • For default, there is no value, as the system will use the specified gateway IP address. • For host, the value is the IP address of the host. • For net, the value is a subnet IP address.
Netmask	For a subnet route, the IP address of the subnet mask.
Gateway	IP address of the gateway.

Create IP routes

Create an IP route.

Note

To change a route, delete it and re-create it with the new settings.

Format
```
/net/route create -if <value> -type {default | host -target
<value> | net -target <value> [-netmask <value>]} [-gateway
<value>]
```

Action qualifier

Qualifier	Description
-if	Type the ID of the interface that the route will use to reach the gateway. View interfaces on page 108 explains how to view the network interface IDs.
	Note
	The system may not use the interface you type for the route. The system determines the best interface for the route automatically.
-type	Type the type of route. Value is one of the following:
	• default — System uses the default gateway when it cannot find a route to a connected node.
	• host — Create a route to a host.
	• net — Create a route to a subnet.
-target	Type the IP address for the target network node based on the value of -type. Value is one of the following:
	• For default, the system will use the IP address specified for -gateway.
	• For host, type the IP address of a target host.
	• For net, type the IP address of a target subnet. Include the -netmask qualifier to specify the IP address of the subnet mask.
-netmask	For a route to a subnet, type the IP address of the subnet mask.
-gateway	Type the gateway IP address for the route.

Example
The following command creates a subnet route on interface IF_1 to target IP address 10.64.74.10:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/route create -if IF_1 -type net -target "10.64.74.10" netmask 255.255.255.0 -gateway "10.64.74.1"

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = RT_1
Operation completed successfully.
```

View IP routes

View details about IP routes. You can filter on the route ID.

Note

The show action command on page 17 explains how to change the output format.

Format
/net/route [-id <value>] show

Object qualifier

Qualifier	Description
-id	Type the ID of a route.

Example

The following command displays details of the IP routes RT_1 and RT_2:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/route show -detail

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID          = rt_0.0.0.0_SPA
        Type        = default
        Target      =
        Netmask     =
        Gateway     = 172.20.1.1
        Interface   = if_2

2:      ID          = rt_Default%fe80::20a:8bff:fe5a:967c_SPA
        Type        = default
        Target      =
        Netmask     =
        Gateway     = fe80::20a:8bff:fe5a:967c
        Interface   = if_6
```

Delete IP routes

Delete an IP route.

Format

/net/route -id <value> delete

Object qualifier

Qualifier	Description
-id	Type the ID of the route to delete.

Example

The following command deletes route RT_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/route -id RT_1 delete

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage link aggregations

Link aggregation lets you link physical ports (for example, port 0 and port 1) on a SP to a single logical port and therefore lets you use up to four Ethernet ports on the SP. If your system has two SPs, and you link two physical ports, the same ports on both SPs are

linked for redundancy. For example, if you link port 0 and port 1, the system creates a link aggregation for these ports on SP A and a link aggregation on SP B.

Each link aggregation is identified by an ID.

Note

The cabling on SP A must be identical to the cabling on SP B, or you cannot configure link aggregation.

Link aggregation has the following advantages:

- Increases overall throughput since two physical ports are linked into one logical port.
- Provides basic load balancing across linked ports since the network traffic is distributed across multiple physical ports.
- Provides redundant ports so that if one port in a linked pair fails, the system does not lose connectivity.

Note

With link aggregation, both linked ports must be connected to the same switch and the switch must be configured to use link aggregation that uses the Link Aggregation Control Protocol (LACP). The documentation that came with your switch should provide more information on using LACP.

The Unisphere online help provides more details on cabling the SPs to the disk-array enclosures (DAEs).

The following table describes the attributes for link aggregation.

Table 35 Link aggregation attributes

Attribute	Description
ID	ID of the link aggregation. The ID is a combination of the link ID and the SP that contains the linked ports.
Ports	IDs of the linked physical ports. The port names include the name of the SP that contains the ports.
SP	Name of the SP on which the ports are linked. Value is SPA or SPB.
MTU size	Maximum transmission unit (MTU) packet size (in bytes) for the linked ports. Default is 1500 bytes per packet.
Requested MTU size	MTU size requested by the user.
Available MTU size	List of available MTU sizes.
Health state	Health state of the link aggregation. The health state code appears in parentheses. Value is one of the following: • `Unknown (0)` — Status is unknown. • `OK (5)` — Working correctly. • `OK BUT (7)` — Lost connection, but the link aggregation is not in use. • `Degraded/Warning (10)` — Working and performing all functions, but the performance may not be optimum.

Table 35 Link aggregation attributes (continued)

Attribute	Description
	• `Minor failure (15)` — Working and performing all functions, but overall performance is degraded. This condition has a minor impact on the system and should be remedied at some point, but does not need to be fixed immediately. • `Major failure (20)` — Failing and some or all functions may be degraded or not working. This condition has a significant impact on the system and should be remedied immediately. • `Critical failure (25)` — Failed and recovery may not be possible. This condition has resulted in data loss and should be remedied immediately. • `Non-recoverable error (30)` — Completely failed and cannot be recovered.
Health details	Additional health information. See Appendix A, Reference on page 367, for health information details.

Create link aggregations

Create a link aggregation by linking two physical ports on an SP to create a logical port.

Note

If your system has two SPs, the specified ports are automatically linked on both SPs for redundancy.

Format
```
/net/la create –ports <value> [-mtuSize <value>]
```

Action qualifier

Qualifier	Description
`–ports`	Type the IDs of the physical ports to link on the SP. Separate the IDs with a comma. For example, to link ports 0 and 1 on SPA, type: eth0_SPA,eth1_SPA.
`–mtuSize`	Type the MTU size (in bytes) for the linked ports. Default value is 1500. **Note** If you want to support jumbo frames, type 9000.

Example
The following command links port 0 and port 1 on SPA with the default MTU size. The system has two SPs, so port 0 and port 1 on SPB are also linked, which results in two link aggregation IDs:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/la create -
ports "eth0_SPA,eth1_SPA"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = la0_SPA
ID = la0_SPB
Operation completed successfully.
```

View link aggregations

View details about link aggregations. You can filter on the link aggregation ID.

Note

If your system has two SPs, details about the link aggregation configured on each SP appear.

Note

explains how to change the output format.

Format
```
/net/la [-id <value>] show
```

Object qualifier

Qualifier	Description
-id	Type the ID of the link aggregation.

Example
The following command shows the link aggregations on the system, in this case, for both SPA and SPB:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/la show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: ID           = la0_SPA
   SP           = SPA
   Ports        = eth0_SPA,eth1_SPA
   Health state = OK (5)

2: ID           = la0_SPB
   SP           = SPB
   Ports        = eth0_SPB,eth1_SPB
   Health state = OK (5)
```

Change link aggregations

Change the settings of a link aggregation.

Note

If your system has two SPs, the specified link aggregation is updated on both SPs.

Format
```
/net/la -id <value> set [-ports <value>] [-mtuSize <value>]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the link aggregation to change.

Action qualifier

Qualifier	Description
-ports	Type the IDs of the physical ports to link on the SP. Separate the IDs with a comma. For example, to link ports 0 and 1 on SPA, type: eth0_SPA,eth1_SPA
-mtuSize	Type the MTU size (in bytes) for the linked ports. Default is 1500 bytes per packet. **Note** If you want to support jumbo frames, type 9000.

Example

The following command changes the MTU size for link aggregation la0_SPA to 9000 bytes. The system has two SPs, so MTU size is updated for both link aggregation IDs:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/la –id la0_SPA set –mtuSize 9000

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = la0_SPA
ID = la0_SPB
Operation completed successfully.
```

Delete link aggregations

Delete a link aggregation.

Note

If your system has two SPs, the specified bond is deleted from both SPs.

Format
```
/net/la [-id <value>] delete
```

Object qualifier

Qualifier	Description
-id	Type the ID of the link aggregation to delete.

Example

The following command deletes link aggregation la0_SPA. The system has two SPs, so link aggregation la0_SPB is also deleted:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/la -id la0_SPA
delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = la0_SPA
ID = la0_SPB
Operation completed successfully.
```

Manage DNS settings

A domain name server (DNS) is a network service responsible for converting domain names to their corresponding IP addresses. The system uses DNS services to resolve network names and IP addresses for the network services it needs (for example, for NTP and SMTP servers) and so that it can obtain IP addresses for hosts addressed by network names rather than IP addresses.

During the initial system configuration process you must specify the network address of at least one DNS server for resolving hostnames to IP addresses. Later, you can add, delete, or change DNS server settings.

You can configure multiple DNS server domains to specify each domain and IP address of the DNS servers for the system to use. By default, the system uses the top entry in the list as the current DNS. The remaining list provides a hierarchy of DNS servers to use if the first-choice server becomes unavailable. If the first DNS server in the list becomes unavailable, the system proceeds to the next DNS server in the list, and so on. You can also specify default DNS server addresses to indicate which addresses the system will use first.

DNS server addresses are grouped under DNS server domains. Each domain is identified by a domain ID.

⚠ CAUTION

You must configure at least one valid DNS server entry in the domain for the system. Deleting the last DNS entry can disrupt network communication to the device, and potentially interrupt communication between the system and the hosts that use its storage resources.

The following table lists the attributes for DNS domains.

Table 36 DNS domain and server attributes

Attribute	Description
NAS server	ID of the associated NAS server.
Name	Name of the DNS domain.
Auto-configuration enabled	Indicates whether DNS addresses are configured automatically.
Name servers	List of IP addresses that correspond to the name servers in the domain.

Configure DNS settings

Configure the DNS settings for the storage system.

Format
```
/net/dns/config set {-nameServer <value> | -auto | -
noNameServer}
```

Action qualifier

Qualifier	Description
-nameServer	Type a list of DNS server addresses to designate as default addresses. Separate the addresses with a comma. The system uses the addresses in the order in which you type them.
-auto	Set DNS addresses dynamically.
-noNameServer	Clear the list of IP addresses.

Example

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/dns/config set -nameServer "128.222.132.29,128.222.132.32"

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

View default DNS addresses

View the DNS server addresses designated as a default.

Note

The show action command on page 17 explains how to change the output format.

Format
```
/net/dns/config show
```

Example
The following command displays the DNS server addresses:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/dns/config show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1. Auto-configuration enabled = no
   Name servers               =
10.5.3.29,10.5.3.32,2001:db8:170:9400:212:3fff:fe2a:8812
```

View DNS server domains

View details about configured DNS server domains.

Note

explains how to change the output format.

Format
```
/net/nas/dns [-server <value>] show
```

Object qualifier

Qualifier	Description
-server	Type the ID of the associated NAS server.

Example
The following command lists all DNS server domains:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/dns -server nas_1 show

```
[Response]
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:     NAS server   = nas_1
       Name         = domain.one.com
       Name servers = 10.64.74.1,10.64.74.201
```

Configure a DNS domain

Configure a DNS server domain.

Format
```
/net/nas/dns -server <value> set { [-name <value>] [-nameServer
<value>]| -enabled no}
```

Object qualifier

Qualifier	Description
-server	Type the name of the associated NAS server.

Action qualifier

Qualifier	Description
-name	Type the name of the associated NAS server.
-nameServer	Type the IP addresses of the DNS servers. Separate the addresses using a comma.
-enabled	Set the value to no to remove DNS settings for the NAS server. Valid value is no.

Example
The following command deletes the DNS domain domain.two.com:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/dns -server
nas_1 set -name "newdomain.one.com"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage NTP server settings

Note

NTP is not required, but some functionality is unavailable without it.

The system relies on the network time protocol (NTP) as a standard for synchronizing the system clock with other nodes on the network. NTP provides a way of synchronizing clocks of distributed systems within approximately one millisecond of each other. A Windows Active Directory domain controller can operate as a time server if the Windows Time Service is running on it.

Some applications will not operate correctly if the clock on the system is not synchronized with the clock on connected hosts. Configure the system and any connected hosts to use the same time server. Doing so does the following:

- Minimizes the chance that synchronization issues will arise between the system and connected hosts.
- Reduces the difficulty of reconciling timestamps used for log information in the different systems.

Note

When using a NAS server for CIFS network shares, the system cannot access an Active Directory domain unless the system is synchronized within five minutes of the Active Directory controller for the domain where the network shares reside.

You can configure a total of three NTP server addresses for the system. All NTP server addresses are grouped into a single NTP server record. NTP is not required, but some functionality is unavailable without it.

The following table lists the attributes for the NTP server record.

Table 37 NTP server record attributes

Attribute	Description
ID	ID of the NTP server record.
Server	Name or IP address of an NTP server.

Create an NTP server record

Create an NTP server to specify an IP address of each NTP server the system will use.

Note

By default, the first NTP server address you specify will become the primary.

Format
```
/net/ntp/server create -server <value> [-force {noReboot |
allowReboot | allowDU}]
```

Action qualifier

Qualifier	Description
-server	Type the name or IP address of an NTP server.
-force	Accept or decline the system reboot, which may be needed to complete the time change. If the qualifier isn't specified, you will be asked to confirm reboot if it's needed. Valid values are: • noReboot • allowReboot • allowDU **Note** Note: **allowDU** is used if the system is in a degraded state or has one SP (data will be unavailable during its reboot). Otherwise **allowReboot** is used. In silent mode, system will be rebooted if needed.

Example
The following creates an NTP server record that contains NTP server address 0.north-america.pool.ntp.org:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/ntp/server

create -server 0.north-america.pool.ntp.org

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = NTP_0.north-america.pool.ntp.org
Operation completed successfully.
```

View NTP server settings

View details about the NTP server.

Note

explains how to change the output format.

Format
```
/net/ntp/server [-id <value>] show
```

Object qualifier

Qualifier	Description
-id	Type the ID of the NTP server.

Example
The following command displays the NTP server record, which contains two NTP server addresses:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/ntp/server show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID      = NTP_0.north-america.pool.ntp.org
        Server  = 0.north-america.pool.ntp.org

2:      ID      = NTP_1.north-america.pool.ntp.org
        Server  = 1.north-america.pool.ntp.org
```

Configure NTP server settings

Configure the NTP server setting.

Format
```
/net/ntp/server set -addr <value>
```

Action qualifier

Qualifier	Description
-addr	Enter a list of one or more IP addresses or network names of each NTP server to include in the NTP server setting. Separate the addresses with a comma.

Example
The following command adds two IP addresses to the NTP server setting:

```
uemcli -d 10.0.0.1 -u Local/joe -p 12345 /net/ntp/server set -addr
"10.64.75.55,10.64.75.44"
```

Delete NTP server settings

Delete an NTP server record to remove the NTP settings.

Note

If you delete the primary NTP server record, the system automatically determines the NTP server record to use.

Format
```
/net/ntp/server -id <value> delete
```

Action qualifier

Qualifier	Description
-id	Type the ID of the NTP server setting to delete.

Example
The following command deletes NTP server setting NTP_10.5.1.207:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/ntp/server -id
NTP_10.5.1.207 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Manage NIS server domains

The Network Information Service (NIS) consists of a directory service protocol for maintaining and distributing system configuration information, such as user and group information, hostnames, and e-mail aliases to network hosts. For example, to back up data on file system shares, some NDMP products require information from NIS servers to back up file system data.

NIS server addresses are grouped under domains, which are identified by domain IDs.

The following table lists the attributes for NIS servers domains.

Table 38 NIS server domain attributes

Attribute	Description
NAS server	ID of the associated NAS server.
Domain	Name of the NIS server domain.
Servers	List of IP addresses of the NIS servers in the domain.

View NIS server domains

View details about NIS server domains.

Note

The show action command on page 17 explains how to change the output format.

Format
```
/net/nas/nis [-server <value>] show
```

Object qualifier

Qualifier	Description
-server	Type the ID of the associated NAS server

Example
The following command displays details about the NIS server domain:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/nis show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:     NAS server  = nas_0
       Domain      = nis.one.com
       Servers     = nisserver1.one.com,10.64.74.1
```

Change NIS server domains

Add NIS server addresses to an NIS server domain.

Format

```
/net/nas/nis -server <value> set { [-domain <value>] [-ip
<value>] | {-enabled no}}
```

Object qualifier

Qualifier	Description
-server	Type the ID of the associated NAS server

Action qualifier

Qualifier	Description
-domain	Type the NIS domain name.
-ip	Type the IP addresses of the NIS servers to include in the domain. Separate the addresses with a comma.
-enabled	Set the value to no to remove NIS settings for the NAS server. Valid value is no.

Example

The following command adds a new IP address to NIS server domain nis.two.com:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/nis -id
nis.two.com set -ip "10.64.74.200"

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection


Operation completed successfully.
```

Manage SMTP server settings

The system uses the Simple Mail Transport Protocol (SMTP) to e-mail alerts, based on alert severity, of system events to specified e-mail addresses and to EMC support using ConnectEMC (if supported). Once you provide the IP address of the SMTP server to use, you can enable the following features on the system:

- E-mail alerts — The system sends e-mail alerts of system events to the specified IP address when it encounters alert or error conditions. The system uses the first IP address you specify.

- ConnectEMC — The system sends e-mail alerts of system events or errors to EMC support using ConnectEMC. After specifying the SMTP server IP address, enter the IP address for ConnectEMC.

Note

If ESRS is enabled, the system prefers it over ConnectEMC SMTP.

Configure alert settings on page 327 explains how to specify the alert severity of which to e-mail alerts. All IP addresses are grouped under a single SMTP server setting.

The following table lists the attributes for SMTP server settings.

Table 39 SMTP server attributes

Attribute	Description
ID	ID of the SMTP server.
Address	IP address of the SMTP server.

View SMTP server settings

View the IP addresses of the SMTP servers.

Note

The show action command on page 17 explains how to change the output format.

Format
```
/net/smtp [-id <value>] show
```

Object qualifier

Qualifier	Description
-id	Type the ID of an SMTP server.

Example
The following command lists the IP addresses of the two SMTP servers in the setting:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/smtp show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:     ID      = default
       Address = 192.168.0.15

2:     ID      = connectEMC
       Address = 10.64.74.15
```

Configure SMTP server settings

Specify the IP addresses for the SMTP server setting.

Format
```
/net/smtp -id <value> set -addr <value>
```

Object qualifier

Qualifier	Description
-id	Type the ID of an SMTP server for which to specify an IP address.

Action qualifier

Qualifier	Description
-addr	Type the IP address for the SMTP server. Note that the address can be either IPv4 or IPv6.

Example

The following command sets the IP address for the default SMTP server that the system will use:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/smtp -id
default set -addr 10.64.74.16
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage NDMP server settings

The Network Data Management Protocol (NDMP) provides a standard for backing up file servers on a network. NDMP allows centralized applications to back up file servers that run on various platforms and platform versions. NDMP reduces network congestion by isolating control path traffic from data path traffic, which permits centrally managed and monitored local backup operations.

Enable NDMP to use NDMP products for backing up and restoring data on file system storage.

The following table lists the attributes for NDMP servers.

Table 40 NDMP server attributes

Attribute	Description
NAS server	ID of the associated NAS server.
Enabled	Indication of whether NDP is enabled. Value is yes or no.
Username	User name for accessing the NDMP server.
Password	Password for accessing the NDMP server.

View NDMP server settings

View whether NDMP is enabled or disabled.

Note

explains how to change the output format.

Format
```
/net/nas/ndmp [-server <value>] show
```

Object qualifier

Qualifier	Description
-server	Type the ID of the associated NAS server.

Example
The following command displays the NDMP settings, which show that NDMP is enabled:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/ndmp show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      NAS server  = nas_0
        Enabled     = yes

2:      NAS server  = nas_1
        Enabled     = no
```

Configure NDMP server settings

Configure NDMP server settings, which includes enabling or disabling NDMP and changing the password for accessing the NDMP server.

Format
```
/net/nas/ndmp -server <value> set -enabled {yes {-passwd
<value> | -passwdSecure} | no}
```

Object qualifier

Qualifier	Description
-server	Type the ID of the associated NAS server.

Action qualifier

Qualifier	Description
-enabled	Enable NDMP. Value is yes or no. For yes, type the NDMP server password.
-passwd	Type the password for the NDMP server. You must specify the password when enabling NDMP.
-passwdSecure	Specify the password in secure mode - the user will be prompted to input the password and the password confirmation.

Example
The following command enables NDMP:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/ndmp -server nas_0 set -enabled yes -passwd "Password0123"

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Manage LDAP settings

The Lightweight Directory Access Protocol (LDAP) is an application protocol for querying and modifying directory services running on TCP/IP networks. LDAP provides central management for network authentication and authorization operations by helping to centralize user and group management across the network. Integrating the system into an existing LDAP environment provides a way to control user and user group access to the system through Unisphere CLI or Unisphere.

After you configure LDAP settings for the system, you can manage users and user groups, within the context of an established LDAP directory structure. For instance, you can assign access permissions to Unisphere CLI that are based on existing users and groups.

Note

The system uses the LDAP settings only for facilitating control of access to Unisphere CLI and Unisphere, not for access to storage resources.

The following table lists the attributes for LDAP settings.

Table 41 LDAP server attributes

Attribute	Description
ID	ID of the LDAP server.
Name	Name of the LDAP server.
Domain name	Domain name for the LDAP server.
Port	Port number used by the directory server for LDAP communications. By default, LDAP uses port 389, and LDAP over an SSL uses port 636.
Protocol	Indication of whether the LDAP protocol uses SSL for secure network communication. SSL provides encryption and authentication capabilities. SSL encrypts data over the network and provides message and server authentication. Value is one of the following: `ldap` (default) — LDAP without SSL. `ldaps` — LDAP with SSL, which is the default.
Bind DN	Port number used by the directory server for LDAP communications. By default, LDAP uses port 389 and LDAP over SSL uses port 636.
Bind password	Base distinguished name (DN) of the root of the LDAP directory tree. The system uses the DN to bind to the LDAP service and determine where in the LDAP directory tree to begin a search for information. The base DN can be expressed as a fully qualified domain name or in X.509 format by using the attribute dc=. For example, if the fully qualified domain name is mycompany.com, the base DN is expressed as dc=mycompany,dc=com.
User search path	Path to search for users on the directory server. For example: ou=People,dc=lss,dc=emc,dc=com.

Table 41 LDAP server attributes (continued)

Attribute	Description
	Note On an Active Directory server, a default search path is used.
Group search path	Path to search for groups on the directory server. For example: uid=‹name›,ou=people,dc=‹domaincomponent›,or dc=‹domain component›. **Note** On an Active Directory server, a default search path is used.
User ID attribute	Name of the LDAP attribute whose value indicates the user ID. Default value is uid.
Group name attribute	Name of the LDAP attribute whose value indicates the group name. Default value is cn.
User object class	LDAP object class for users. Default is user. In Active Directory, groups and users are stored in the same hierarchical directory path and the class is called group.
Group object class	LDAP object class for groups. Default value is group. In Active Directory, groups and users are stored in the same directory path and the class is called group.
Group member class	Name of the LDAP attribute whose value contains names of group members within a group. Default value is member.
Certificate filepath	Path to the trusted certificate file used for one-way LDAP server authentication.
LDAP timeout	Timeout for the LDAP server in milliseconds. If the system does not receive a reply from the LDAP server after the specified timeout, it stops sending requests. Default value is 30,000 milliseconds, or 30 seconds.

Configure LDAP settings

Configure LDAP settings to control user access to Unisphere CLI and Unisphere from an LDAP server.

Format
```
/net/ldap create -name <value> –domain <value> [-port <value>]
[-protocol {ldap|ldaps -certFilePath <value>}] –bindDn <value>
{-bindPasswd <value> | -bindPasswdSecure} [-userSearchPath
<value>] [-groupSearchPath <value>] [-userIdAttr <value>] [-
groupNameAttr <value>] [-userObjectClass <value>] [-
groupObjectClass <value>] [-groupMemberAttr <value>] [-timeout
<value>]
```

Action qualifier

Qualifier	Description
-name	Type the IP address or hostname of the primary directory server to use for authentication. The value you type depends on the format of the subject field entry in the directory server's certificate. Typically, this requires a hostname.
-domain	Type the domain name for the LDAP server.
-protocol	Specify whether the LDAP protocol uses SSL for secure network communication. SSL provides encryption and authentication capabilities. SSL encrypts data over the network and provides message and server authentication. Value is one of the following: • `ldap` (default) — LDAP without SSL. • `ldaps` — LDAP with SSL, which is the default.
-certFilePath	Type the path to the trusted certificate file used for one-way server authentication. **Note** If the value of -protocol is ldaps, this qualifier is required.
-port	Type the port number used by the directory server for LDAP communications. By default, LDAP uses port 389, and LDAP over an SSL uses port 636.
-bindDn	Type the base distinguished name (DN) of the root of the LDAP directory tree. The system uses the DN to bind to the LDAP service and determine where in the LDAP directory tree to begin a search for information. The base DN can be expressed as a fully-qualified domain name or in X.509 format by using the attribute dc=. For example, if the fully-qualified domain name is mycompany.com, the base DN is expressed as dc=mycompany,dc=com.
-bindPasswd	Type the password to be used for binding to the LDAP server.
-bindPasswdSecure	Specify the password in secure mode - the user will be prompted to input the password.
-userSearchPath	Type the path to search for users on the directory server. For example: ou=People,dc=lss,dc=emc,dc=com **Note** On an Active Directory server, a default search path is used.
-groupSearchPath	Type the path to search for groups on the directory server. For example: ai.uid=‹name›,ou=people,dc=‹domaincomponent›,or dc=‹domain component›.

Qualifier	Description
	Note On an Active Directory server, a default search path is used.
-userIdAttr	Type the name of the LDAP attribute whose value indicates the user ID. Default value is uid.
-groupNameAttr	Type the LDAP object class for users. Default value is user. In Active Directory, groups and users are stored in the same hierarchical directory path and the class is called group.
-groupObjectClass	Type the LDAP object class for groups. Default value is group. In Active Directory, groups and users are stored in the same directory path and the class is called group.
-groupMemberAttr	Type the name of the LDAP attribute whose value contains names of group members within a group. Default value is member.
-timeout	Type the timeout for the LDAP server in milliseconds. If the system does not receive a reply from the LDAP server after the specified timeout, it stops sending requests. Default is 30,000 milliseconds, or 30 seconds.

Example

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/ldap create -name lpso242.lss.emc.com -domain local -port 389 -protocol ldap -bindDn "cn=Directory Manager" -bindPasswd Password0123 -userSearchPath "ou=People,dc=lss,dc=emc,dc=com" -groupSearchPath "ou=Groups,dc=lss,dc=emc,dc=com" -userIdAttr "uid" -groupNameAttr "cn" -userObjectClass "interOrgPerson" -groupObjectClass "groupOfUniqueNames" -groupMemberAttr "uniqueMember" -timeout 40000

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = LDAP_1
Operation completed successfully.
```

View LDAP settings

View details for configured LDAP settings.

Note

The show action command on page 17 explains how to change the output format.

Format
`/net/ldap [-id <value>] show`

Object qualifier

Qualifier	Description
-id	Type the ID of the LDAP setting.

Example

The following command displays the LDAP settings:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/ldap show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID              = LDAP_1
        Server name     = lpso242.lss.emc.com
        Domain          = local
        Protocol        = ldap
        Port            = 389
```

Change LDAP settings

Update a configured LDAP setting.

Format

```
/net/ldap -id <value> set [-name <value>] [-port <value>] [-
protocol {ldap | ldaps {-certFilePath <value>}}] [-bindDn
<value>] [-bindPasswd <value> | -bindPasswdSecure] [-
userSearchPath <value>] [-groupSearchPath <value>] [-userIdAttr
<value>] [-groupNameAttr <value>] [-userObjectClass <value>] [-
groupObjectClass <value>] [-groupMemberAttr <value>] [-timeout
<value>]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the LDAP setting to change.

Action qualifier

Qualifier	Description
-name	Type the name for the LDAP server.
-domain	Type the domain name for the LDAP server.
-port	Type the port number used by the directory server for LDAP communications. By default, LDAP uses port 389, and LDAP over an SSL uses port 636.
-protocol	Type whether the LDAP protocol uses SSL for secure network communication. SSL provides encryption and authentication capabilities. SSL encrypts data over the network and provides message and server authentication. Value is one of the following: • ldap (default) — LDAP without SSL. • ldaps — LDAP with SSL, which is the default.
-certFilePath	Type the path to the trusted certificate file used for one-way server authentication.

Qualifier	Description
–bindDn	Type the base distinguished name (DN) of the root of the LDAP directory tree. The system uses the DN to bind to the LDAP service and determine where in the LDAP directory tree to begin a search for information. The base DN can be expressed as a fully qualified domain name or in X.509 format using the attribute dc=. For example, if the fully qualified domain name is mycompany.com, the base DN is expressed as dc=mycompany,dc=com.
–bindPasswd	Type the password to be used for binding to the LDAP server. This qualifier is required when the –bindDn qualifier is included.
–bindPasswdSecure	Specifies the password in secure mode - the user will be prompted to input the password.
–userSearchPath	Type the path to search for users on the directory server. For example: ou=People,dc=lss,dc=emc,dc=com. **Note** On an Active Directory server, a default search path is used.
–groupSearchPath	Type the path to search for groups on the directory server. For example: uid=‹name›,ou=people,dc=‹domaincomponent›,or dc=‹domain component›. **Note** On an Active Directory server, a default search path is used.
–userIdAttr	Type the name of the LDAP attribute whose value indicates the user ID. Default value is uid.
–groupNameAttr	Type the name of the LDAP attribute whose value indicates the group name. Default value is cn.
–userObjectClass	Type the LDAP object class for users. Default value is user. In Active Directory, groups and users are stored in the same hierarchical directory path and the class is called group.
–groupObjectClass	Type the LDAP object class for groups. Default value is group. In Active Directory, groups and users are stored in the same directory path and the class is called group.
–groupMemberAttr	Name of the LDAP attribute whose value contains names of group members within a group. Default value is member.
–timeout	Type the timeout for the LDAP server in milliseconds. If the system does not receive a reply from the LDAP server after the specified timeout, it stops sending requests. Default is 30000 milliseconds, or 30 seconds.

Example

The following command updates the configured LDAP settings:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/ldap -id lDAP_1
set –server lpso242.lss.emc.com –port 389
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = LDAP_1
Operation completed successfully.
```

Verify LDAP settings

Verify the connection to the LDAP server.

Format
/net/ldap –id <*value*> verify

Object qualifier

Qualifier	Description
-id	Identifies the LDAP server.

Example
The following command verifies the connection to the LDAP server:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/ldap –id LDAP_1
verify
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Delete LDAP settings

Delete an LDAP setting.

Format
/net/ldap –id <*value*> delete

Object qualifier

Qualifier	Description
-id	Type the ID of the LDAP setting to delete.

Example
The following command deletes the LDAP_1 setting:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/ldap –id LDAP_1
delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Utility commands

Ping allows you to check connectivity between your system and a remote host. You may select the interface from which to ping. The system automatically identifies the SP to which the selected interface belongs.

Traceroute allows you to check the network route from the specified interface to a remote host. You may select the interface and the host address that are the endpoints of the route.

Ping

Ping a remote host from the specified interface (−srcIf parameter value).

Format
`/net/util/ping -srcIf <value> -addr <value>`

Action qualifier

Qualifier	Description
−srcIf	Identifies the interface from which the packet will be sent. The value shall be an interface identifier.
−addr	Specify the destination address to use when sending the packet.

Example
The following example pings a remote host:

uemcli /net/util ping -srcIf if_0 -addr 10.5.2.183

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully
```

Trace route

Display the route from the specified interface to a remote host

Format
`/net/util/traceroute -srcIf <value> -addr <value>`

Action qualifier

Qualifier	Description
−srcIf	Identifies the interface from which the packet will be sent. The value shall be an interface identifier.
−addr	Specify the destination address to use when sending the packet.

Example
The following example pings a remote host:

uemcli /net/util/traceroute -srcIf if_0 -addr 10.5.2.183

```
Storage system address: 10.0.0.1
Storage system port: 443
```

```
HTTPS connection

1: Result = traceroute to 10.64.74.57 (10.64.74.57), 30 hops max, 40
byte packets using UDP

2: Result =  1  10.64.76.2 (10.64.76.2)  0.944 ms   0.801 ms   0.808
ms

3: Result =  2  10.64.74.57 (10.64.74.57)  0.431 ms   0.473 ms
0.354 ms
```

Manage advanced storage access

Advanced storage access is required by the vCenter Plug-in application. The Advanced storage access feature allows the VCenter Plug-in user to perform advanced file system functions.

The following table lists the attributes for Advanced storage access.

Table 42 Advanced storage access attributes

Attribute	Description
NAS server	NAS server ID.
State	The state of the Advanced storage access service. Valid values are: • Disabled • Enabled **Note** Values are case-insensitive.
Username	The Advanced storage access user name.
Password	The Advanced storage access user password.

View Advanced storage access settings

Displays Advanced storage access settings.

Format
```
/net/nas/asa [-server <value>] show
```

Object qualifier

Qualifier	Description
-server	Type the ID of the associated NAS server

Example
The following command displays the Advanced storage access settings:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/asa show

```
Storage system address: 10.0.0.1
Storage system port: 443
```

```
HTTPS connection

1:    NAS server  = nas_0
      State       = Enabled
```

Change Advanced storage access settings

Modifies the Advanced storage access settings.

Format
```
/net/nas/asa -server <value> set [-state {Disabled | Enabled}]
[-passwd <value> | -passwdSecure]
```

Object qualifier

Qualifier	Description
-server	Type the ID of the associated NAS server

Action qualifier

Qualifier	Description
-state	Specifies whether the Advanced storage access service is enabled. Possible values include: • `Disabled` — Advanced storage access service is disabled. • `Enabled` — Advanced storage access service is enabled.
-passwd	Specifies the Advanced storage access user password. **Note** This attribute is mandatory if the current state is being changed from Disabled to EnabledPerHost or EnabledForAll.

Example
The following command changes the Advanced storage access password:

uemcli /net/nas/asa -server nas_0 set -state Enabled -passwd newpassword

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

CHAPTER 4

Manage Hosts

This chapter addresses the following topics:

Manage host configurations

Hosts are the clients or servers in your network that access storage on the system. Host configurations are logical connections through which hosts or applications can access storage resources. Before a host can access storage, you must define a configuration for it and associate it with a storage resource. Create a host configuration for each host, host subnetwork (subnet), or network group (netgroup) that will access storage resources on the system.

You can create the following types of host configurations:

- Individual host configurations — Enable you to define and control access to storage resources on a host-by-host basis.

- Subnet and netgroup configurations — Enable you to define and control access to storage resources for multiple hosts or network segments.

For hosts that will access iSCSI storage, create an iSCSI port to specify the iSCSI initiator settings and assign it to a host configuration. Manage host initiators on page 149 explains how to configure iSCSI initiators for host configurations.

Each host configuration is identified by an ID.

The following table lists the attributes for host configurations.

Table 43 Host configuration attributes

Attribute	Description
ID	ID of the host configuration.
Name	Name of the host configuration.
Description	Brief description of the host configuration.
Address	Hostname or IP address associated with the host, IP address of the subnet, or network address of the netgroup. **Note** This information is required when connecting hosts to network shares on the system.
Netmask	Subnet mask for the host.
Type	Type of host configuration. Value is one of the following: • `host` — Define and control access to storage resources on a host-by-host basis. • `subnet` — A subnet is a logical grouping of connected network devices. Devices on a subnet share contiguous ranges of IP addresses. For IPv4 networks, a subnet mask, or network mask, defines the boundaries of an IP subnet. The prefix length, specified as a component of the `-addr` parameter, defines the boundaries of an IPv6 subnet. • You can associate a host configuration with a subnet mask to define and control storage access for hosts on a particular network segment. • `netgroup` — A netgroup is a named sets of hosts, users, or domains on a network. A netgroup can provide a way to reference sets of Linux/UNIX hosts collectively for accessing storage over NFS.

Table 43 Host configuration attributes (continued)

Attribute	Description
	• You can create a host configuration for a netgroup to define and control storage access for multiple Linux/UNIX hosts or users through a single configuration. **Note** Typically, netgroups are accessible only through NIS. If NIS is not running, netgroups are not defined. Manage NIS server domains on page 124 explains how to configure NIS server communication.
OS type	Type of operating system (OS) that runs on the host or netgroup. Value is one of the following: • undefined — OS is not specified (default). • other — OS is unknown. • win2003srv — Windows Server 2003. • winxp — Windows XP. • win2008srv — Windows Server 2008. • winvista — Windows Vista. • redhat — Red Hat Linux Enterprise. • sles — Suse Linux Enterprise. • win7 — Windows 7 • hyperv — Microsoft Hyper-V • solaris — Solaris 10 SPARC • win2012srv — Windows Server 2012
Ignored address	A comma-separated list of host IP addresses to exclude from data access.
Health state	Health state of the system. The health state code appears in parentheses. Value is one of the following: • Unknown (0) — Status is unknown. • OK (5) — Working correctly. • OK BUT (7) — Working correctly, but there could be a problem. • Degraded/Warning (10) — Working and performing all functions, but the performance may not be optimum. • Minor failure (15) — Working and performing all functions but overall performance is degraded. This condition has a minor impact on the system and should be remedied at some point, but does not have to be fixed immediately. • Major failure (20) — Failing and some or all functions may be degraded or not working. This condition has a significant impact on the system and should be remedied immediately.

Table 43 Host configuration attributes (continued)

Attribute	Description
	• `Critical failure (25)` — Failed and recovery may not be possible. This condition has resulted in data loss and should be remedied immediately. • `Non-recoverable error (30)` — Completely failed and cannot be recovered.
`Health details`	Additional health information. See Appendix A, Reference, for health information details.
`Management type`	Indicates the way the host is managed. Value is one of the following: • `VMware` — The host is managed through VMware web services. • `Others` — The host is automatically created on the storage system. • `Manual` — The host is created manually.

Create host configurations

Create a host configuration to establish a connection between the system and hosts that access the system.

Format

```
/remote/host create -name <value> [-descr <value>] -type {host
-addr <value> [-ignoredAddr <value>] [-osType {undefined |
other | win2003srv | winxp | win2008srv | winvista | win2012srv
| esx | redhat | sles} ] | subnet -addr <value> [-netmask
<value>] | netgroup -addr <value>}
```

Action qualifier

Qualifier	Description
`-name`	Specifies the name of the host configuration.
`-descr`	Specifies a brief description of the host configuration.
`-addr`	Specifies the hostnames or IP addresses associated with the host, IP addresses of the subnet, or the network addresses of the netgroup. Separate each value with a comma. Format: *‹IP address›*/[*‹prefix length›*]. Default prefix length for IPv4 addresses is 24 and IPv6 addresses is 64. **Note** This information is required when connecting hosts to network shares on the system.
`-type`	Specifies the type of host configuration. Value is one of the following: • `host` — A host defines and controls access to storage resources on a host-by-host basis. • `subnet` — A subnet is a logical grouping of connected network devices. Devices on a subnet share contiguous ranges of IP

Qualifier	Description
	addresses. A subnet mask, or network mask, defines the boundaries of an IP subnet. You can associate a host configuration with a subnet mask to define and control storage access for hosts on a particular network segment. • `netgroup` — A netgroup is a named sets of hosts, users, or domains on a network. A netgroup can provide a way to reference sets of Linux/UNIX hosts collectively for accessing storage over NFS. You can create a host configuration for a netgroup to define and control storage access for multiple Linux/UNIX hosts or users through a single configuration. **Note** Typically, netgroups are only accessible through NIS. If NIS is not running, netgroups are not defined. Manage NIS server domains on page 124 explains how to configure NIS server communication.
`-ignoredAddr`	Specifies a list of IP addresses associated with the host that are excluded from data access. Separate each value with a comma.
`-netmask`	Specifies the subnet mask for the host configuration.
`-osType`	Specifies the type of operating system (OS) running on the host or netgroup. Value is one of the following: • `Undefined` — OS is not specified (default). • `other` — OS is unknown. • `win2003srv` — Windows Server 2003. • `winxp` — Windows XP. • `win2008srv` — Windows Server 2008. • `winvista` — Windows Vista. • `win2012srv` — Windows Server 2012. • `esx` — VMware ESX. • `redhat` — Red Hat Linux Enterprise. • `sles` — SUSE Linux Enterprise. • `win7` — Windows 7. • `hyperv` — Microsoft Hyper-V. • `solaris` — Solaris 10 SPARC.

Example 1

The following command creates a host configuration for a host with these settings:

- Name is MyHost.
- Description is "accounting".
- IP address is 10.64.74.10.

- OS is Windows XP.

The host configuration receives ID 1014:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/host create
-name MyHost -descr "accounting" -type host -addr 10.64.74.10 -osType
winxp
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = 1014
Operation completed successfully.
```

Example 2

The following command creates a host configuration for a subnet with these settings:

- Name is MySubnet.
- Description is "subnet1".
- IP address is 192.168.10.0.
- Subnet mask is 255.255.255.0.

The host configuration receives ID 1015:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/host create
-name MySubnet -descr "subnet1" -type subnet -addr 192.168.10.0 -
netmask 255.255.255.0
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = 1015
Operation completed successfully.
```

Example 3

The following command creates a host configuration for a subnet with these settings:

- Name is IPv6Subnet.
- Description is "V6_HE_Subnet".
- IPv6 address is 2001:db8:c25:
- Prefix length is 48.

The host configuration receives ID 1023:

```
uemcli -d 10.0.0.1 /remote/host create -name IPv6Subnet -descr
"V6_HE_Subnet" -type subnet -addr 2001:db8:c25::/48
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = 1023
Operation completed successfully.
```

View host configurations

View details about a host configuration. You can filter on the ID of the host configuration or the host type.

Format
```
/remote/host [{-id <value>|-type {host|subnet|netgroup}}] show
```

Object qualifier

Qualifier	Description
-id	Identifies the host configuration.
-type	Specifies the host type. Value is one of the following: host, subnet, or netgroup.

Example
The following command lists all host configurations on the system:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/host show -detail

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID              = 1014
        Name            = MyHost
        Description     = this is my host
        Type            = host
        Address         = 10.64.74.10, 10.64.80.10
        Netmask         =
        OS type         = winxp
        Ignored address = 10.64.80.10
        Health state    = OK (5)

2:      ID              = 1015
        Name            = MySubnet
        Description     = this is my subnet
        Type            = subnet
        Address         = 192.168.10.0
        Netmask         = 255.255.255.0
        OS type         =
        Ignored address =
        Health state    = OK (5)
```

Change host configuration settings

Change the settings for a host configuration.

Format
```
/remote/host -id <value> set [-name <value>] [-descr <value>]
[-addr <value>] [-ignoredAddr <value>] [ [-netmask <value>] | -
osType {undefined | other | win2003srv | winxp | win2008srv |
winvista | win2012srv | esx | redhat | sles} } ]
```

Object qualifier

Qualifier	Description
-id	Identifies the host configuration to change.

Action qualifier

Qualifier	Description
-name	Specifies the new name for the host configuration.
-desc	Specifies the new description of the host configuration.
-addr	Specifies the hostnames or IP addresses associated with the host, IP addresses of the subnet, or the network addresses of the netgroup. Separate each value with a comma. • For subnet type, specifies the new IP address of the subnet. • For netgroup, specifies the new netgroup's network address. • Format: *‹IP address›*/[*‹prefix length›*]. • Default prefix length of IPv6 is 64. **Note** This information is required when connecting hosts to network shares on the system.
-ignoredAddr	Specifies a list of IP addresses associated with the host that are excluded from data access. Separate each value with a comma.
-netmask	Specifies the subnet mask IP address for the host configuration.
-osType	Specify the type of operating system (OS) running on the host or netgroup. Value is one of the following: • undefined — OS is not specified (default) . • other — OS is unknown. • win2003srv — Windows Server 2003. • winxp — Windows XP. • win2008srv — Windows Server 2008. • winvista — Windows Vista. • win2012srv — Windows Server 2012. • esx — VMware ESX. • redhat — Red Hat Linux Enterprise. • sles — SUSE Linux Enterprise. • win7 — Windows 7. • hyperv — Microsoft Hyper-V. • solaris — Solaris 10 SPARC.

Example
The following command updates the description of host configuration 1014 to indicate that it now holds the payroll database:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/host -id
1014 set -descr "Accounting" -osType winxp
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = 1014
Operation completed successfully.
```

Delete host configurations

Delete a host configuration.

⚠ **CAUTION**

Deleting a host configuration breaks the iSCSI-based storage connections associated with the configuration. Hosts that use the configuration for NFS-based storage connections, such as NFS shares, revert to the default access privileges for any storage resources that they can access.

Format
```
/remote/host -id <value> delete
```

Object qualifier

Qualifier	Description
-id	Identifies the host configuration to delete.

Example
The following command deletes host configuration 1014:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/host -id
1014 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage host LUNs

Host LUNs are the storage resources that belong to the hosts connected to the storage system.

There are two types of host LUNs:

- Production LUNs— Read/write LUNs used for data access..
- Snapshot LUNs — Read-only snapshots of a production LUN.

Each host LUN is identified by an ID.

The following table lists the attributes for host LUNs.

Table 44 Host LUN attributes

Attribute	Description
Host	ID of the host that owns the LUN.
Host name	Name of the host that owns the LUN.
LUN	Friendly ID of the LUN.
LUN type	LUN type. Value is one of the following: • Snap • Production
LUN name	LUN name
LUN ID	Logical unit number on the host, or the host LUN ID.

View host LUN configurations

View details about a host LUN. You can filter on the ID of the host, the ID of the LUN, or the LUN type.

Note

The show action command on page 17 explains how to change the output format.

Format

```
/remote/host/hlu { -host <value> | -lun <value> | -host <value>
-lun <value> } [-type { production | snap } ] show
```

Object qualifier

Qualifier	Description
-host	Specifies the host ID.
-lun	Specifies the LUN ID.
-type	Specifies the LUN type.

Example

The following command lists all host LUNs on host 1043:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/host/hlu -
host 1043 show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      Host     = 1043
        LUN      = lun_112
        LUN type = production
        LUN ID   = 3
```

Change host LUN configuration settings

Change the host LUN ID.

Note

This operation will fail if you try to assign a LUN ID that is already in use.

Format

```
/remote/host/hlu -host <value> -lun <value> -type { production
| snap } set -lunId <value>
```

Object qualifier

Qualifier	Description
-host	Specifies the host ID.
-lun	Specifies the LUN ID.
-type	Specifies the LUN type.

Action qualifier

Qualifier	Description
-lunId	Specifies the new LUN ID for the LUN on the selected host.

Example

The following command changes the ID of LUN 1058 on host 1043 to LUN 0:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/host/hlu -
host 1043 -lun 1058 -type production set -lunId 0
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage host initiators

After you create a host configuration for controlling host access to storage on the system, you need to create an initiator for each host configuration that accesses the storage system. The initiator represents the initiator on the host, which will connect to the storage system. There are two types of initiators, Fibre Channel (FC) and iSCSI.

An FC initiator contains the World Wide Name (WWN) of the host.

An iSCSI initiator contains a name for the host, its iSCSI address (an iSCSI initiator IQN), and, optionally, the CHAP authentication password associated with the host. Manage reverse CHAP for mutual CHAP authentication on page 89 explains how to configure reverse (two-way) CHAP authentication on the system..

Each initiator is identified by an ID.

The following table lists the attributes for initiators.

Table 45 Initiator attributes

Attribute	Description
ID	Host initiator ID.

Table 45 Initiator attributes (continued)

Attribute	Description
Host	Name of the parent host.
UID	FC WWN or iSCSI IQN of the initiator.
Initiator type	The type of initiator. Value is one of the following: • FC • iSCSI
Ports logged in	Comma-separated list of array target ports that the initiator is logged into.
Ignored	Indicates whether the initiator is ignored for data access to the host. Value is one of the following: • Yes — The initiator is ignored. • No — The initiator is not ignored.
Health state	Health state of the system. The health state code appears in parentheses. Value is one of the following: • Unknown (0) — Status is unknown. • OK (5) — Working correctly. • OK BUT (7) — Working correctly, but there could be a problem. • Degraded/Warning (10) — Working and performing all functions, but the performance may not be optimum. • Minor failure (15) — Working and performing all functions but overall performance is degraded. This condition has a minor impact on the system and should be remedied at some point, but does not have to be fixed immediately. • Major failure (20) — Failing and some or all functions may be degraded or not working. This condition has a significant impact on the system and should be remedied immediately. • Critical failure (25) — Failed and recovery may not be possible. This condition has resulted in data loss and should be remedied immediately. • Non-recoverable error (30) — Completely failed and cannot be recovered.
Health details	Additional health information. See Appendix A, Reference, for health information details.
CHAP users	List of CHAP accounts configured for the initiator.

Create iSCSI initiators

Create an FC or iSCSI initiator and assign it to a host configuration.

Format
```
/remote/initiator create –host <value> -uid <value> -type
{iscsi|fc}
```

Object qualifier

Qualifier	Description
-host	Identifies the host configuration to which to assign the initiator. View host configurations on page 144 explains how to view the IDs of host configurations on the system.
-uid	Specifies the FC WWN or the iSCSI IQN of the host to which to assign the initiator.
-type	Specifies the type of initiator. Value is one of the following: • iscsi • fc

Example

The following command creates an iSCSI initiator for host configuration 1014. The iSCSI initiator receives ID ISCSII_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/initiator

create -host 1014 -uid "20:00:00:00:C9:29:0F:FD:

10:00:00:00:C9:29:0F:FD" -type fc
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = 1021
Operation completed successfully.
```

View initiators

View a list of initiators. You can filter on the initiator ID, host ID, or whether the initiator is registered.

Note

The show action command on page 17 explains how to change the output format.

Format
```
/remote/initiator [{-id <value> | -host <value> | -
unregistered}] show
```

Object qualifier

Qualifier	Description
-id	Identifies the initiator.
-host	Type the ID of a host configuration to view the initiators assigned to the host configuration.
-unregistered	Specifies unregistered initiators.

Example

The following command lists all initiators on the system:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/initiator show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: ID             = 1058
   Host           = 1014
   UID            = iqn.1991-05.com.microsoft:nlpc20971
   Initiator type = iscsi
   Ports logged in = eth1_SPA, eth1_SPB
   Ignored        = false no
   Health state   = OK (5)
```

Modify initiators

Modify an already created initiator.

Format

```
/remote/initiator -id <value> set [-ignored {yes | no}] [-host <value>]
```

Object qualifier

Qualifier	Description
-id	Specifies the ID of the initiator

Action qualifier

Qualifier	Description
-ignored	Specifies whether the initiator is ignored for data access to the host. Value is one of the following: • Yes — The initiator is ignored. • No — The initiator is not ignored.
-host	Identifies the host configuration to which the initiator is assigned. View host configurations on page 144 explains how to view the IDs of host configurations on the system

Example

The following command assigns initiator 1058 to host 1014:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/initiator -id 1058 set -host 1014

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage host initiator paths

The storage system communicates with a host initiator over a host initiator path. The storage system uses this path to identify the host initiator configuration information.

The following table lists the attributes for a host initiator path.

Table 46 Initiator path attributes

Attribute	Description
Initiator	Parent initiator.
Port	The ID of the target port.
Logged in	Indicates whether the initiator path is logged in. Value is one of the following: • Yes • No
Host	The host ID to which the initiator path is registered. No value in this field means the initiator is not registered to a host. **Note** This host ID may be different from that of the initiator when auto-push registration and initiator registration information are not the same. This causes the storage system to generate an alert.
Registration method	Indicates how the initiator path is registered. Value is one of the following: • Unknown — The initiator was registered by a method other than ESX push. • ESX — ESX pushed the initiator registration to the storage system.
Session IDs	Comma-separated list of the session IDs for this path.
Health state	Health state of the system. The health state code appears in parentheses. Value is one of the following: • Unknown (0) — Status is unknown. • OK (5) — Working correctly. • OK BUT (7) — Working correctly, but there could be a problem. • Degraded/Warning (10) — Working and performing all functions, but the performance may not be optimum. • Minor failure (15) — Working and performing all functions but overall performance is degraded. This condition has a minor impact on the system and should be remedied at some point, but does not have to be fixed immediately. • Major failure (20) — Failing and some or all functions may be degraded or not working. This condition has a significant impact on the system and should be remedied immediately.

Table 46 Initiator path attributes (continued)

Attribute	Description
	• `Critical failure (25)` — Failed and recovery may not be possible. This condition has resulted in data loss and should be remedied immediately. • `Non-recoverable error (30)` — Completely failed and cannot be recovered.
`Health details`	Additional health information. See Appendix A, Reference on page 367, for health information details.

View initiator paths

View a list of initiators. You can filter on the initiator ID.

Note

explains how to change the output format.

Format
```
/remote/initiator/path [-initiator <value>] show
```

Object qualifier

Qualifier	Description
`-initiator`	Type the ID of the initiator to display the paths associated with it.

Example
The following command lists all initiator paths on the system:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/initiator/`
`path show`

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:     Initiator    = 1043
       Port         = eth1_SPB
       Logged in    = Yes
       Host         = 1014
       Health state = OK (5)
```

Manage iSCSI CHAP accounts for one-way CHAP authentication

The system uses a CHAP account to authenticate a host (initiator) attempting to access an iSCSI storage resource (target). CHAP authentication can be one of the following:

• One-way, where only the target authenticates the initiator. To set one-way CHAP authentication, create a CHAP account for a host configuration that access iSCSI storage.

• Reverse (also called mutual or two-way), where the target and initiator authenticate each other. Compared to one-way CHAP, enabling reverse CHAP provides an extra level of security. To set reverse CHAP, specify a reverse secret password. Manage

explains how to configure reverse CHAP authentication.

Each CHAP account is identified by an ID.

The following table lists the attributes for CHAP accounts.

Table 47 CHAP Account Attributes

Attribute	Description
ID	ID of the CHAP account.
IQN	IQN address of the host (initiator).
Wildcard	Whether this is wildcard CHAP, where all initiators can be authenticated by the storage system. Value is one of the following: • Yes — All initiators can be authenticated by the storage system. • No — Authentication is on a per initiator basis.
Username	CHAP username.
Secret	CHAP secret password.
Secret format	The CHAP input format. Value is one of the following: • ASCII — ASCII format • Hex — Hexadecimal format

Create iSCSI CHAP accounts

Create an iSCSI CHAP account for a host (initiator).

Format
```
/remote/iscsi/chap create {-iqn <value> | -wildcard} [-username
<value>] {-secret <value> | -secretSecure} [ -secretFormat
{ ascii | hex } ]
```

Object qualifier

Qualifier	Description
-iqn	Specifies the IQN address of the host (initiator).
-wildcard	Specifies whether this is a wildcard CHAP, where all initiators can be authenticated by the storage system.
-username	Specifies the CHAP username.
-secret	Specifies the CHAP secret password.
-secretSecure	Specifies the CHAP secret in secure mode - the user will be prompted to input the password.
-secretFormat	Specifies the CHAP input format. Value is one of the following: • ASCII — ASCII format • Hex — Hexadecimal format Default value is ASCII format.

Example

The following command creates an iSCSI CHAP account for a host. It receives the ID CHAP_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/iscsi/chap
create -iqn iqn.1991-05.com.microsoft:cpc7745 -secret opqrstuvwxyz
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = CHAP_1
Operation completed successfully.
```

View iSCSI CHAP accounts

View details about iSCSI CHAP accounts on the system.

Note

The show action command on page 17 explains how to change the output format.

Format
```
/remote/iscsi/chap [-id <value>] show
```

Object qualifier

Qualifier	Description
-id	Identifies the iSCSI CHAP account.

Example

The following command displays all iSCSI CHAP accounts on the system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/iscsi/chap
show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID       = CHAP_1
        IQN      = iqn.1991-05.com.microsoft:cpc7745
        Wildcard = no
        Username = iqn.1991-05.com.microsoft:cpc7745

2:      ID       = CHAP_2
        IQN      =
        Wildcard = yes
        Username = globalChapUserName
```

Change iSCSI CHAP account settings

Change the settings for an iSCSI CHAP account, such as the secret password.

Format
```
/remote/iscsi/chap -id <value> set [-username <value>]{-secret
<value> | -secretSecure} [ -secretFormat { ascii | hex } ]
```

Object qualifier

Qualifier	Description
-id	Identifies the iSCSI CHAP account to change.

Action qualifier

Qualifier	Description
-username	Specifies the CHAP username.
-secret	Specifies the CHAP secret password.
-secretSecure	Specifies the CHAP secret in secure mode - the user will be prompted to input the password.
-secretFormat	Specifies the CHAP input format. Value is one of the following: • ASCII — ASCII format • Hex — Hexadecimal format

Example

The following command updates the secret password for iSCSI CHAP account CHAP_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/iscsi/chap -
id CHAP_1 set -secret abcdef123456
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Delete iSCSI CHAP accounts

Delete an iSCSI CHAP account.

Note

If you delete an iSCSI CHAP account, the host that used it will no longer be authenticated when attempting to access iSCSI storage.

Format

```
/remote/iscsi/chap -id <value> delete
```

Object qualifier

Qualifier	Description
-id	Type the ID of the CHAP account to delete.

Example

The following command deletes iSCSI CHAP account CHAP_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/iscsi/chap -
id CHAP_1 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
```

```
HTTPS connection

Operation completed successfully.
```

Manage VMware virtual center

Manage VMware vCenter servers.

The following table lists the attributes for VMFS datastores.

Table 48 VMware virtual center attributes

Attribute	Description
ID	ID of the VMware virtual center
Address	Domain name or IP address of VMware vCenter.
User name	Name of the user account on the VMware vCenter.
Password	Password of the user account on the VMware vCenter.
Description	Description of the VMware vCenter.

Create VMware virtual center

Adds the virtual center credentials. The virtual center credentials are stored in the storage system. In order to execute this command, the user must have account on the storage system.

Format

```
/virt/vmw/vc create -addr <value> -username <value> {-passwd
<value> | -passwdSecure} [ -descr <value> ]
```

Action qualifier

Qualifier	Description
-addr	Domain name or IP address or domain name of the VMware vCenter.
-username	Specifies the username used to access the VMware vCenter.
-passwd	Specifies the password used to access the VMware vCenter.
-passwdSecure	Specifies the password in secure mode - the user will be prompted to input the password.
-descr	Specifies the description of the VMware vCenter server.

Example

The following command adds virtual center credentials:

uemcli /virt/vmw/vc create -address 10.14.12.209 -username root -passwd xxx -descr "Add virtual center"

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = VC_1
Operation completed successfully
```

Set the credentials or description of an existing virtual center

Modifies the credentials or description of the existing virtual center. In order to execute this command the user must have account on the storage system.

Format
```
/virt/vmw/vc -id <value> set [-addr <value>] [-username <value>
{-passwd <value> | -passwdSecure} ] [-descr <value>]
```

Object qualifier

Qualifier	Description
-id	Identifies the VMware vCenter server.

Action qualifier

Qualifier	Description
-addr	Specifies the new IP address or domain name of the VMware vCenter server.
-username	Specifies the username.
-passwd	Specifies the password.
-passwdSecure	Specifies the password in secure mode - the user will be prompted to input the password.
-descr	Specifies the new description of the VMware vCenter server.

Example
The following command specifies the new description of the VMware center:

uemcli /virt/vmw/vc -id VC_1 set -descr "This vCenter manages 2 ESX servers"

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = VC_1
Operation completed successfully.
```

Delete an existing virtual center

Removes an existing virtual center. In order to execute this command the user must have account on the storage system.

Format
```
vc -id <value> delete
```

Object qualifier

Qualifier	Description
-id	Identifies the VMware vCenter server.

Example

The following example deletes an existing virtual center.

uemcli /virt/vmw/vc -id VC_1 delete

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully
```

View all virtual centers

Displays a list of configured VMware vCenter servers.

Format
/virt/vmw/vc [-id <*value*>] show

Object qualifier

Qualifier	Description
-id	Identifies the VMware vCenter server.

Example

The following example shows a list of all virtual centers.

uemcli /virt/vmw/vc show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:     ID          = VC_1
       Address     = 10.14.12.241
       Description = This vCenter manages 2 ESX servers
```

Refresh all virtual centers

Rescan details of all configured VMware Vcenter servers.

Format
/virt/vmw/vc refresh [-scanHardware]

Object qualifier

Qualifier	Description
-scanHardware	Specify to rescan hardware changes also (takes additional time).

Example

The following example rescans all virtual centers.

```
uemcli /virt/vmw/vc refresh -scanHardware
```

```
[Response]
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage ESX server

Manage VMware ESX servers.

The following table lists the attributes for ESX server.

Table 49 ESX server attributes

Attribute	Description
ID	ID of the ESX server.
Name	Name of the ESX server.
Address	Domain name or IP address of ESX server.
Virtual center	Identifier of the VMware VCenter containing the server.
Username	Name of the user account on the ESX server.
Password	Password of the user account on the ESX server.
Description	Description of the ESX host.

Create an ESX server

Adds a VMware ESX server.

Format
```
/virt/vmw/esx create -addr <value> { -vc <value> | -username
<value> {-passwd <value> | -passwdSecure} } [ -descr
<value> ] ] [ -resolveConflicts { yes | no } ]
```

Action qualifier

Qualifier	Description
-addr	Domain name or IP address of the ESX server.
-vc	Identifies the VMware vCenter server.
-username	Specifies the username used to access the VMware ESX server.
-passwd	Specifies the password used to access the VMware ESX server.
-passwdSecure	Specifies the password in secure mode - the user will be prompted to input the password.
-descr	Specifies the description of the VMware ESX server.

Qualifier	Description
-resolveConflicts	Specifies the option to resolve IP address or initiator conflicts interactively. Valid values are yes or no (default).

Example 1

uemcli /virt/vmw/esx create -addr 10.14.12.209 -username root -passwd xxx -descr "My ESX server"

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = ESX_1
Operation completed successfully
```

Example 1 Example

uemcli /virt/vmw/esx create -addr 10.14.12.219 -vc VMwareVC_12 -resolveConflicts yes

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

The ESX host to be created has IP addresses and/or Initiators already
present in an existing host.
The ID of the existing host is: Host_12
The IP addresses in conflict are: 10.14.12.219, 10.14.12.220
The Initiators in conflicts are: iqn.1998-01.com.vmware:test1-1, iqn.
1998-01.com.vmware:test1-2

WARNING, the existing host has IP addresses and/or Initiators not
found in the ESX host to be created. If you continue with the ESX
host creation, those IP addresses and/or Initiators will be removed
and can no longer be used for storage access.
The IP address not in the ESX host are: 10.14.12.217, 10.14.12.218
The Initiators not in the ESX host are: iqn.1998-01.com.vmware:test1-3

Do you want to convert the existing host to the ESX host?
Yes / no:yes

ID = ESX_1
Operation completed successfully
```

Change ESX server credentials

Changes ESX server credentials and/or description. In order to execute this command the user must have account on the storage system.

Format
```
/virt/vmw/esx -id <value> set [ -descr <value> ] [ -username
<value> { -passwd <value> | -passwdSecure } ] [ -addr <value> ]
```

Object qualifier

Qualifier	Description
-id	Identifies the VMware ESX server.

Action qualifier

Qualifier	Description
-descr	Specifies the comment or description.
-username	Specifies the username used to access the VMware ESX server.
-passwd	Specifies the password used to access the VMware ESX server.
-passwdSecure	Specifies the new password in secure mode - the user will be prompted to input the password.
-addr	Specifies the domain name or IP address of the ESX server for Unisphere to contact the ESX server directly. **Note** This is only applicable to standalone ESX servers.

Example

uemcli /virt/vmw/esx -id ESX_1 set -descr "Changing ESX Server description"

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = ESX_1
Operation completed successfully.
```

Delete ESX server credentials

Deletes ESX server credentials.

Format
```
/virt/vmw/esx -id <value> delete
```

Object qualifier

Qualifier	Description
-id	Identifies the ESX server.

Example

uemcli /virt/vmw/esx -id ESX_1 delete

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

View all existing ESX servers

Displays a list of all configured VMware ESX servers.

Format
```
/virt/vmw/esx [{ -id <value> | -vc <value> }] show
```

Object qualifier

Qualifier	Description
-id	Identifies the VMware ESX server.
-vc	Identifies the VMware vCenter server.

Example

uemcli /virt/vmw/esx -vc VC_1 show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID      = ESX_1
        Name    = nlpc12240.us.dg.com
        vCenter = VC_1
        Address = 10.14.12.240

2:      ID      = ESX_2
        Name    = nlpc12241.us.dg.com
        vCenter = VC_1
        Address = 10.14.12.241
```

Discover all ESX Servers

Lists all VMware ESX servers on the specified VMware vCenter server.

Format

```
/virt/vmw/esx discover { -vc <value> | -vcAddr <value> -
username <value> {-passwd <value> | -passwdSecure} } [ -
createAll ]
```

Action qualifier

Qualifier	Description
-vc	Identifies the existing VMware vCenter.
-vcAddr	IP address or domain name of the VMware vCenter.
-username	Specifies the name of the VMware vCenter.
-passwd	Specifies the password of the VMware vCenter
-passwdSecure	Specifies the password in secure mode - the user will be prompted to input the password.
-createAll	Adds all discovered ESX servers automatically.

Example

uemcli /virt/vmw/esx discover -vc VC_1

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      Name    = nlpc12240.us.dg.com

2:      Name    = nlpc12241.us.dg.com
```

```
Operation completed successfully
```

Refresh an ESX server

Rescans details of a VMware ESX server.

Format
```
/virt/vmw/esx [-id <value>] refresh [-scanHardware]
```

Object qualifier

Qualifier	Description
-id	Identifies the ESX server. If ID is not specified, rescan all virtualization objects.

Action qualifier

Qualifier	Description
-scanHardware	Specify to rescan hardware changes also (takes additional time).

Virtual machine

Manage VMware virtual machines.

The following table lists the attributes for Virtual machine.

Table 50 Virtual machine attributes

Attribute	Description
ID	ID of the virtual machine.
Name	Name of the virtual machine
Description	Description of the virtual machine.
ESX server	ESX server containing the virtual machine.
OS	Guest operating system.
State	Virtual machine power state. Valid values are: • Powered on • Powered off • Suspended

View all existing virtual machines

Displays a list of all existing virtual machines on the existing ESX servers.

Format
```
/virt/vmw/vm [ -id <value> | -esx <value> ] show
```

Object qualifier

Qualifier	Description
-id	Identifies the virtual machine.
-esx	Identifies the ESX server.

Example

uemcli /virt/vmw/vm -esx ESX_1 show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID          = VM_1
        Name        = WinVM1
        vCenter     = VC_1
        ESX server  = ESX_1
        State       = Powered On

2:      ID          = VM_2
        Name        = LinVM3
        vCenter     = VC_1
        ESX server  = ESX_1
        State       = Suspended
```

VM hard disk

Manage hard disk properties for VMware virtual machines

The following table lists the attributes for VM hard disks.

Table 51 VM hard disk attributes

Attribute	Description
Name	Name of the hard disk.
Type	Type of the VM hard disk.
Capacity	VM hard disk capacity.
Datastore	Associated datastore.

View all hard disks

Displays hard disk properties for a specified virtual machine.

Format
/virt/vmw/vmdevice -vm <*value*> show

Object qualifier

Qualifier	Description
-vmId	Identifies the virtual machine.

Example

`uemcli /virt/vmw/vmdevice -vm VM_1 show`

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      Name      = Hard disk 1
        Type      = VM Hard Disk
        Capacity  = 107374182400 (100GB)
        Datastore = Storage1

2:      Name      = Hard disk 2
        Type      = VM Hard Disk
        Capacity  = 107374182400 (100GB)
        Datastore = Storage1
```

CHAPTER 5

Manage Hardware Components

This chapter addresses the following topics:

Manage Storage Processor (SP)

The following table lists the health state values for the storage processor (SP) in Normal mode.

Table 52 Storage processor health state values (Normal mode)

Code	Health state	Reason(s)
0	Unknown	• The health of the component cannot be determined.
5	OK	• The SP is operating normally.
10	Degraded/Warning	• The write cache is disabled on the SP. • The SP is starting.
20	Major failure	• The SP has faulted. • The SP is missing. • The SP is not responding.

The following table lists the health state values for the storage processor in Service/ Rescue mode.

Table 53 Storage processor health state values (Service/Rescue mode)

Code	Health state	Reason(s)
0	Unknown	• The health of the component cannot be determined.
10	Degraded/ Warning	• A user has placed the SP into the Service mode.
20	Major failure	• The system software on this SP has encountered a problem. • The CPU in the SP has faulted. • IO module 0 in the SP has faulted. • IO module 1 in the SP has faulted. • The CPU and IO module 0 in the SP have faulted. • The CPU and IO module 1 in the SP have faulted. • Memory DIMM 0 in the SP has faulted. • Memory DIMM 0 and 1in the SP have faulted. • Memory DIMM 1 in the SP has faulted. • Memory DIMM 2 in the SP has faulted. • Memory DIMMs in the SP have faulted. • The SP has faulted. • The SSD in the SP has faulted. • The entire blade in the SP has faulted. • The fibre cable connection in the SP has faulted.

Table 53 Storage processor health state values (Service/Rescue mode) (continued)

Code	Health state	Reason(s)
		• The enclosure in the SP has faulted.
		• An I/O module in the SP is configured incorrectly.
		• An unexpected error has occurred in the SP.
		• A cable is in the wrong SAS port on the SP.
		• No SAS port was found on the SP.
		• There is an invalid disk configuration on the SP
		• There is no I/O between ab I/O module in the SP and a link control card on a disk array enclosure.
		• A FLARE DB disk in the storage processor has faulted.
		• One of the first four disks have mismatched types.
		• One of the first four disks have an invalid block size.
		• One of the first four disks have mismatched size.
		• DPE resume is missing an EMC serial number.

View Storage Processor

View existing Storage Processors (SPs).

Format
```
/env/sp [-id <value>] show
```

Object qualifier

Qualifier	Description
-id	Identifies the Storage Processor.

Example 1 (physical deployments only)
The following command displays the existing SPs:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/sp show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: ID          = spa
   DPE         = DPE_1
   Slot        = 1
   Mode        = Normal
   Health state = OK (5)
   Memory size  = 34359738368 (32G)

2: ID          = spb
   DPE         = DPE_1
   Slot        = 2
   Mode        = Normal
   Health state = OK (5)
   Memory size  = 34359738368 (32G)
```

Example 2 (virtual deployments only)

The following command displays existing SP for a virtual system.

```
uemcli -d 10.0.0.2 -u Local/joe -p MyPassword456! /env/sp show -detail
```

```
Storage system address: 10.0.0.2
Storage system port: 443
HTTPS connection

1:     ID             = spa
       DPE            = dpe
       Slot           = 0
       Name           = SP A
       Mode           = Normal
       Health state   = OK (5)
       Health details = "The component is operating normally. No
action is required."
       Model          = VIRT SP 12GB
       Memory size    = 12884901888 (12.0G)
```

Manage disk

The following table lists the health state values for the disk.

Table 54 Disk health state values

Code	Health state	Reason(s)
0	Unknown	• The health of the component cannot be determined.
5	OK	• The disk is operating normally. • The disk slot is empty.
10	Degraded/ Warning	• The disk is resynchronizing with the system. • The disk cannot be used because the system has exceeded the maximum number of allowable disks.
15	Minor failure	• The disk is inserted in the wrong slot. • The disk is removed. • The disk is offline.
20	Major failure	• The disk has faulted. • The disk is unsupported.

View disk

View existing disks.

Format
```
/env/disk [ {-id <value> | -pool <value> | -fastcache | -
unused} ] show
```

Object qualifier

Qualifier	Description
-id	ID of the disk.
-pool	Shows the disks that belong to the specified pool.
-fastcache	Shows the disks used in FAST Cache.
-unused	Shows unused disks.

Example

The following command displays the existing disks:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/disk show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID                 = DISK_0
        Enclosure          = DAE_1
        Slot               = 0
        Health state       = OK (5)
        User capacity      = 2199023255552 (2T)
        Used by FAST Cache = no
        Pool ID            = pool_1

2:      ID                 = DISK_1
        Enclosure          = DAE_1
        Slot               = 1
        Health state       = OK (5)
        User capacity      = 2199023255552 (2T)
        Used by FAST Cache = no
        Pool ID            = pool_1
```

Rescan disk (virtual deployments only)

Rescan the system for available virtual disks.

Format

```
/env/disk rescan [-async]
```

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.

Example

The following command rescans the system for hot-plugged virtual disks.

uemcli -d 10.0.0.2 -u Local/joe -p MyPassword456! /env/disk rescan

```
Storage system address: 10.0.0.2
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage battery (physical deployments only)

The following table lists the health state values for the system batteries.

Table 55 Battery health state values

Code	Health state	Reason(s)
0	Unknown	• The health of the component cannot be determined.
5	OK	• The battery is operating normally.
10	Degraded/Warning	• The battery is charging.
20	Major failure	• The battery has faulted. • The battery is missing.

View battery

View a list of system batteries.

Format
```
/env/bat [-id <value>] show
```

Object qualifier

Qualifier	Description
-id	ID of the battery.

Example
The following command displays a list of system batteries:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/bat show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:        ID            = Bat_0
          SP            = SPA
          Slot          = 0
          Health state  = OK (5)

2:        ID            = Bat_0
          SP            = SPA
          Slot          = 1
          Health state  = Degraded/Warning (10)
```

Manage power supply (physical deployments only)

The following table lists the health state values for system power supplies.

Table 56 Power supply health state values

Code	Health state	Reason(s)
0	Unknown	• The health of the component cannot be determined.
5	OK	• The power supply is operating normally.
20	Major failure	• The power supply has faulted. • The power supply is not receiving power. • The power supply has been removed.

View power supply

View a list of system power supplies.

Format
```
/env/ps [-id <value>] show
```

Object qualifier

Qualifier	Description
-id	ID of the power supply.

Example
The following command displays a list of system power supplies:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/ps show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:          ID            = Pow_0
            Enclosure     = DPE
            SP            = SPA
            Slot          = 0
            Health state  = OK (5)

2:          ID            = Pow_1
            Enclosure     = DPE
            SP            = SPA
            Slot          = 1
            Health state  = OK(5)
```

Manage link control card (LCC) (physical deployments only)

The following table lists the health state values for system link control cards (LCCs).

Table 57 Link control card health state values

Code	Health state	Reason(s)
0	Unknown	• The health of the component cannot be determined.

Table 57 Link control card health state values (continued)

Code	Health state	Reason(s)
5	OK	• The LCC is operating normally.
20	Major failure	• The LCC has faulted. • The LCC has been removed.

View link control card

View a list of LCCs.

Format
```
/env/lcc [-id <value>] show
```

Object qualifier

Qualifier	Description
-id	ID of the LCC.

Example
The following command displays a list of system LCCs:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/lcc show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: ID           = LCC_0
   DAE          = DAE_0
   Slot         = 0
   Health state = OK (5)

2: ID           = LCC_1
   DAE          = DAE_0
   Slot         = 1
   Health state = OK(5)
```

Manage SSD (physical deployments only)

The following table lists the health state values for system SSDs.

Table 58 SSD health state values

Code	Health state	Reason(s)
0	Unknown	• The health of the component cannot be determined.
5	OK	• The SSD is operating normally.
10	Degraded/Warning	• The SSD is failing.
20	Major failure	• The SSD has failed.

Table 58 SSD health state values (continued)

Code	Health state	Reason(s)
		• The SSD has been removed.

View SSD

View a list of system SSDs.

Format
```
/env/ssd [-id <value>] show
```

Object qualifier

Qualifier	Description
-id	ID of the SSD.

Example
The following command displays a list of system SSDs:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/ssd show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:       ID           = SSD_0
         SP           = SPA
         Slot         = 0
         Health state = OK (5)

2:       ID           = SSD_1
         SP           = SPA
         Slot         = 1
         Health state = OK(5)
```

Manage disk array enclosure (DAE)

The following table lists the health state values for system disk array enclosures (DAEs).

Table 59 Disk array enclosure health state values

Code	Health state	Reason(s)
0	Unknown	• The health of the component cannot be determined.
5	OK	• The DAE is operating normally.
7	OK_BUT	• The DAE is adjusting the communication speed.
10	Degraded/Warning	• The DAE performance is degraded.
20	Major failure	• The DAE has a disk drive- type mismatch. • The DAE has taken a communication fault.

Table 59 Disk array enclosure health state values (continued)

Code	Health state	Reason(s)
		• The DAE has faulted. • The DAE has a faulted LCC. • The DAE has been misconfigured. • The DAE has been miscabled. • The DAE has been removed. • The DAE had taken a power fault. • The DAE is connected to a faulted I/O module.

View disk array enclosure

View a list of system DAEs.

Format
```
/env/dae [-id <value>] show
```

Object qualifier

Qualifier	Description
-id	ID of the DAE.

Example
The following command displays a list of system DAEs:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/dae show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:        ID           = DAE_0
          Slot         = 0
          Health state = OK (5)

2:        ID           = DAE_1
          Slot         = 1
          Health state = OK(5)
```

Manage disk processor enclosure (DPE)

The following table lists the health state values for system disk processor enclosures (DPEs).

Table 60 Disk processor enclosure health state values

Code	Health state	Reason(s)
0	Unknown	• The health of the component cannot be determined.

Table 60 Disk processor enclosure health state values (continued)

Code	Health state	Reason(s)
5	OK	• The DPE is operating normally.
7	OK_BUT	• The DPE is adjusting the communication speed.
10	Degraded/ Warning	• The DPE performance is degraded.
20	Major failure	• The DPE has a disk drive-type mismatch. • The DPE has taken a communication fault. • The DPE has faulted. • The DPE has a faulted LCC. • The DPE has been misconfigured. • The DPE has been miscabled. • The DPE has been removed. • The DPE had taken a power fault. • The DPE is connected to a faulted I/O module. • The DPE has taken an inter-processor control fault and needs to be recovered. • The DPE has taken an inter-processor communication fault and needs to be recovered.

View disk processor enclosure

View a list of system DPEs.

Format
```
/env/dpe [-id <value>] show
```

Object qualifier

Qualifier	Description
-id	ID of the DPE.

Example 1 (physical deployments only)
The following command displays a list of system DPEs:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/dpe show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:        ID           = DPE_0
          Slot         = 0
          Health state = OK (5)

2:        ID           = DPE_1
```

```
              Slot          = 1
              Health state = OK(5)
```

Example 2 (virtual deployments only)

The following command displays a list of system DPEs:

**uemcli -d 10.0.0.2 -u Local/joe -p MyPassword456! /env/dpe show -
detail**

```
Storage system address: 10.0.0.2
Storage system port: 443
HTTPS connection

1:    ID                    = dpe
      Slot                  = 0
      Name                  = DPE
      Health state          = OK (5)
      Health details        = "The component is operating normally.
No action is required."
      Manufacturer          = VMware
      Model                 = VIRT SINGLE SP DPE 16
```

Manage memory module (physical deployments only)

The following table lists the health state values for system memory modules.

Table 61 Memory module health state values

Code	Health state	Reason(s)
0	Unknown	• The health of the component cannot be determined.
5	OK	• The memory module is operating normally.
20	Major failure	• The memory module has faulted. • The memory module has been removed.

View memory module

View a list of system memory modules.

Format
/env/mm [-id <*value*>] show

Object qualifier

Qualifier	Description
-id	ID of the memory module.

Example
The following command displays a list of system memory modules:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/mm show

```
Storage system address: 10.0.0.1
Storage system port: 443
```

```
HTTPS connection

1:      ID           = MM_SPA_0
        SP           = SPA
        Slot         = 0
        Health state = OK (5)

2:      ID           = MM_SPA_1
        SP           = SPA
        Slot         = 1
        Health state = OK (5)
```

Manage cache card

The following table lists the health state values for the system cache cards.

Table 62 System cache card health state values

Code	Heath state	Reason(s)
0	Unknown	• The health of the component cannot be determined.
5	OK	• The cache protection module is operating normally.
10	Degraded/Warning	• The cache protection module is degraded.
20	Major failure	• The cache protection module has been removed. • The cache protection module has faulted.

View cache card module

View a list of system cache cards.

Format
```
/env/ccard [-id <value>] show
```

Object qualifier

Qualifier	Description
-id	Identifies the system cache card.

Example
The following command displays a list of system cache cards:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/ccard show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:         ID           = CCard_0
           Slot         = 0
           Health state = OK (5)
```

Manage fan modules (physical deployments only)

The following table lists the health state values for the system fan modules.

Table 63 System fan module health state values

Code	Health state	Reason(s)
0	Unknown	• The health of the component cannot be determined.
5	OK	• The fan module is operating normally.
10	Degraded/Warning	• The fan module is degraded.
20	Major failure	• The fan module has been removed. • The fan module has faulted.

View fan module

View a list of system fan modules.

Format
```
/env/fan [-id <value>] show
```

Object qualifier

Qualifier	Description
-id	Identifies the fan module.

Example
The following command displays a list of system cache cards:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/fan show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID           = Fan_0
        DPE          = DPE_0
        Slot         = 0
        Health state = OK (5)

2:      ID           = Fan_1
        DPE          = DPE_0
        Slot         = 1
        Health state = Degraded/Warning (10)
```

Manage I/O modules (physical deployments only)

I/O modules provide connectivity between the SPs and the disk-array enclosure. You can view details about each I/O module installed in the system, such as the health state. Commit a newly added I/O module to configure it for use by the system. Each I/O module record and alert is identified by an ID. The following table lists the attributes for I/O modules.

Table 64 I/O module attributes

Attribute	Description
ID	ID of the I/O module.
SP	ID of the SP to which the I/O module is connected.
Slot	Disk-processor enclosure (DPE) slot in which the I/O module is installed.
Name	Name of the I/O module.
Manufacturer	Manufacturer of the I/O module.
Model	Model of the I/O module.
Health state	Health state of the I/O module. The health state code appears in parentheses. Value is one of the following: • Unknown (0) — Unable to determine the health of the I/O module. • OK (5) — I/O module is operating normally. • Degraded/Warning (10) — I/O module has not been committed (configured). Commit I/O modules on page 183 explains how to commit an I/O module. • Minor failure (15) — One or both of the following may have occurred: • ▪ I/O module has not been committed (configured) after a rebooting the SP. ▪ I/O module is installed in the wrong slot. • Major failure (20) — One or both of the following may have occurred: ▪ I/O module has been removed. Re-install the I/O module. ▪ I/O module has faulted and needs to be replaced. The Unisphere online help explains how to order a replacement I/O module. ▪ I/O module is misconfigured. Commit the I/O module to re-configure it.
Health details	Additional health information. See Appendix A, Reference, for health information details.
Part number	EMC Part Number on the I/O module.
Serial number	EMC Serial Number on the I/O module.

Commit I/O modules

When you add a new I/O module to the system, you must first commit it before the system can use it. The system automatically commits unconfigured I/O modules.

Format
```
/env/iomodule commit
```

Example

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/iomodule commit

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

View I/O modules

View details about I/O modules in the system. You can filter on the I/O module ID.

Note

provides more details on changing the output format.

Format
/env/iomodule [-id <*value*>] show

Object qualifier

Qualifier	Description
-id	Enter the ID of an I/O module.

Example
The following command displays details about the two I/O modules in the system:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/iomodule show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:     ID           = IO_SPA_0
       SP           = SPA
       Slot         = 0
       Health state = OK (5)

2:     ID           = IO_SPA_1
       SP           = SPA
       Slot         = 1
       Health state = Degraded/Warning (10)
```

CHAPTER 6

Manage Storage

This chapter addresses the following topics:

Configure storage pools automatically (physical deployments only)

Storage pools are the groups of disks, called disk groups, on which you create storage resources. The system can automatically configure storage pools by selecting the appropriate disk groups based on the type and availability of disks in the system. Configure custom storage pools on page 188 explains how to configure custom storage pools.

Note

Before you create storage resources, you must configure at least one storage pool.

The following table lists the attributes for automatic pool configuration.

Table 65 Automatic pool configuration attributes

Attribute	Description

Target	Type of disk configuration. Value is one of the following:
	
	• `pool` - Disks configured in a pool.
	
	• `spares` - Disks assigned to storage pools as spares. The number of spares assigned to a pool is dependent on the disk type and pool type:
	
	  ■ For Capacity pools, no spare disks are assigned.
	
	  ■ For Performance pools, a spare disk is assigned for the first 0-30 disks, and then another spare disk is assigned for every group of thirty disks after that.
	
	  ■ For Flash pools, a spare disk is assigned for the first 0-30 disks, and then another spare disk is assigned for every group of thirty disks after that.

Name	Name of the pool. The system allocates disks to one or more of the following pools based on the types and characteristics of the disks on the system: • `Capacity` - Storage allocated from near-line (NL) serial attached SCSI (SAS) disks. Provides high-capacity storage, but with lower overall performance to regular SAS and Enterprise Flash Drive (EFD) disks. Use NL SAS disks to provide extremely economical storage for operations, such as data backup, that do not require high I/O performance. • `Performance` - Storage allocated from serial attached SCSI (SAS) disks. Provides medium performance and medium capacity storage for applications that require balance of performance and capacity. • `Flash` - Storage allocated from EFD disks. Extremely high level performance, but at a relatively high cost per GB of storage. EFDs are most applicable to applications that require high I/O performance and energy efficiency. Depending on the pool type, the system configures the disks into different RAID groups and assigns disks to pools as spares. The Unisphere online help provides more details about storage pools and spares.

Table 65 Automatic pool configuration attributes (continued)

Attribute	Description
Drives (current)	List of disks currently in the pool.
Drives (new)	List of disks to be added to the pool.
RAID level	RAID level applied.
Stripe length	Comma-separated list of disks in the stripe.

Initiate automatic storage pool configuration

Start configuring storage pools automatically. View configuration settings for automatic storage pool creation on page 187 displays the configuration settings that the system will apply when you run this command.

Format
/stor/config/auto set

Action qualifier

Qualifier	Description
-async	Run action in asynchronous mode.

Example
The following command initiates automatic storage pool configuration:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/auto set

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

View configuration settings for automatic storage pool creation

View the settings for automatic storage pool creation that will be applied to the system. Initiate automatic storage pool configuration on page 187 explains how to apply these settings to the system.

Note

The show action command on page 17 explains how to change the output format.

Format
/stor/config/auto show

Example
The following command shows how storage pools and spares will be configured automatically on the system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/auto
show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   Target          = Pool
     Name            = Performance
     Drives (current) = 5 x 600GB SAS; 5 x 300GB SAS
     Drives (new)    = 5 x 600GB SAS
     RAID level      = 5
     Stripe length   = 5,9

2:   Target          = Pool
     Name            = Capacity
     Drives (current) = 10 x 1TB NL-SAS
     Drives (new)    = 2 x 1TB NL SAS
     RAID level      = 5
     Stripe length   = 5,9

3:   Target          = Pool
     Name            = Extreme Performance
     Drives (current) = 10 x 100GB EFD
     Drives (new)    = 10 x 100GB EFD
     RAID level      = 1
     Stripe length   = 2

4:   Target          = Spares
     Name            = Unused / Hot Spare Candidates
     Drives (current) = 1 x 600GB SAS; 1 x 300GB SAS; 1 x 1TB NL SAS
     Drives (new)    = 1 x 100GB EFD
     RAID level      =
     Stripe length   =
```

Configure custom storage pools

Storage pools are the groups of disks on which you create storage resources. Configure storage pools based on the type of storage resource and usage that will be associated with the pool, such as file system storage optimized for database usage. The storage characteristics differ according to the following:

- Type of disk used to provide the storage.

- RAID level implemented for the storage.

Note

Before you create storage resources, you must configure at least one storage pool.

Configure storage pools automatically (physical deployments only) on page 186 explains how to have the system configure storage pools automatically.

The following table lists the attributes for storage pools:

Table 66 Custom storage pool attributes

Attribute	Description
ID	ID of the storage pool.
Name	Name of the storage pool.
Description	Brief description of the storage pool.

Table 66 Custom storage pool attributes (continued)

Attribute	Description
`Total space`	Total storage capacity of the storage pool.
`Current allocation`	Amount of storage in the storage pool allocated to storage resources.
`Remaining space`	Amount of storage in the storage pool not allocated to storage resources.
`Subscription`	For thin provisioning, the total storage space subscribed to the storage pool. All storage pools support both standard and thin provisioned storage resources. For standard storage resources, the entire requested size is allocated from the pool when the resource is created, for thin provisioned storage resources only incremental portions of the size are allocated based on usage. Because thin provisioned storage resources can subscribe to more storage than is actually allocated to them, storage pools can be over provisioned to support more storage capacity than they actually possess. **Note** The system automatically generates an alert when the total pool usage reaches 85% of the pool's physical capacity. – `alertThreshold` specifies the alert threshold value.
`Subscription percent`	For thin provisioning, the percentage of the total space in the storage pool that is subscription storage space.
`Alert threshold`	Threshold for the system to send an alert when hosts have consumed a specific percentage of the subscription space. Value range is 50 to 85.
`Drives`	List of the types of disks on the system, including the number of disks of each type, in the storage pool.
`Number of drives`	Total number of disks in the storage pool.
`Number of unused drives`	Number of disks in the storage pool that are not being used.
`RAID level` (physical deployments only)	RAID level of the disks in the storage pool.
`Stripe length` (physical deployments only)	Number of disks the data is striped across.
`Rebalancing`	Indicates whether a pool rebalancing is in progress. Value is one of the following: ● `Yes` ● `No`
`Rebalancing progress`	Indicates the progress of the pool rebalancing as a percentage.
`System defined pool`	Indication of whether the system configured the pool automatically. Valid values are: ● `Yes`

Table 66 Custom storage pool attributes (continued)

Attribute	Description
	• `No`
`Health state`	Health state of the storage pool. The health state code appears in parentheses. Value is one of the following:
	• `Unknown (0)` - Health is unknown.
	• `OK (5)` - Operating normally.
	• `OK BUT (7)` - Pool has exceeded its user-specified threshold or the system specified threshold of 85%.
	• `Degraded/Warning (10)` - Pool is operating, but degraded due to one or more of the following:
	▪ Pool has exceeded the user-specified threshold.
	▪ Pool is nearing capacity.
	▪ Pool is almost full.
	▪ Pool performance has degraded.
	• `Major failure (20)` - Dirty cache has made the pool unavailable.
	• `Critical failure (25)` - Pool is full. To avoid data loss, add more storage to the pool, or create more pools.
	• `Non-recoverable error (30)` - Two or more disks in the pool have failed, possibly resulting in data loss.
`Health details`	Additional health information. See Appendix A, Reference, for health information details.
`FAST Cache enabled`	Indicates whether FAST Cache is enabled on the storage pool. Value is one of the following:
	• `Yes`
	• `No`
`Protection size used`	Quantity of storage used for data protection.
`Auto-delete state`	Indicates the state of an auto-delete operation on the storage pool. Value is one of the following:
	• `Idle`
	• `Running`
	• `Could not reach LWM`
	• `Could not reach HWM`
	Note If the auto-delete operation cannot satisfy the high water mark, and there are snapshots in the storage pool, the auto-delete operation sets the auto-delete state for that watermark to Could not reach HWM , and generates an alert.

Table 66 Custom storage pool attributes (continued)

Attribute	Description
	• `Failed`
`Auto-delete paused`	Indicates whether an auto-delete operation is paused. Value is one of the following: • `Yes` • `No`
`Auto-delete pool full threshold enabled`	Indicates whether the system will check the pool full high water mark for auto-delete. Value is one of the following: • `Yes` • `No`
`Auto-delete pool full high water mark`	The pool full high watermark on the storage pool.
`Auto-delete pool full low water mark`	The pool full low watermark on the storage pool.
`Auto-delete snapshot space used threshold enabled`	Indicates whether the system will check the snapshot space used high water mark for auto-delete. Value is one of the following: • `Yes` • `No`
`Auto-delete snapshot space used high water mark`	High watermark for snapshot space used on the storage pool.
`Auto-delete snapshot space used low water mark`	Low watermark for snapshot space used on the storage pool.

Configure storage pools

Configure a storage pool.

Format

```
/stor/config/pool create [-async] -name <value> [-descr
<value>] {-diskGroup <value> -drivesNumber <value> -storProfile
<value> | -disk <value> [-tier <value>]} [-alertThreshold
<value>] [-snapPoolFullThresholdEnabled {yes|no}] [ -
snapPoolFullHWM <value>] [-snapPoolFullLWM <value>] [-
snapSpaceUsedThresholdEnabled {yes|no}] [-snapSpaceUsedHWM
<value>] [-snapSpaceUsedLWM <value>]
```

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-name`	Type a name for the storage pool.
`-descr`	Type a brief description of the storage pool.
`-storProfile` (physical deployments only)	Type the ID of the storage profiles, separated by commas, to apply to the storage pool, based on the type of storage resource that will use the pool and the intended usage of the pool. View storage profiles (physical deployments only) on page 213 explains how to view the IDs of available storage profiles on the system. If this option is not specified, a default RAID configuration is selected for each particular drive type in the selected disk group: NL-SAS (RAID 6 with a stripe length of 8), SAS (RAID 5 with a stripe length of 5), or Flash (RAID 5 with a stripe length of 5).
`-diskGroup` (physical deployments only)	Type the IDs of the disk groups to use in the storage pool. Specifying disk groups with different disks types causes the creation of a multi-tier storage pool. View disk groups on page 215 explains how to view the IDs of the disk groups on the system.
`-drivesNumber` (physical deployments only)	Specify the disk numbers, separated by commas, from the selected disk groups to use in the storage pool. If this option is specified when `-storProfile` is not specified, the operation may fail when the `-drivesNumber` value does not match the default RAID configuration for each drive type in the selected disk group.
`-disk` (virtual deployments only)	Specify the list of disks, separated by commas, to use in the storage pool. Specified disks must be reliable storage objects that do not require additional protection.
`-tier` (virtual deployments only)	Specify the list of tiers, separated by commas, to which the disks are assigned. If a tier is omitted, it will be assigned automatically if tiering information for the associated disk is available. Valid values include: • `capacity` • `performance`

Qualifier	Description
	• extreme
-alertThreshold	For thin provisioning, specify the threshold, as a percentage, when the system will alert on the amount of subscription space used. When hosts consume the specified percentage of subscription space, the system sends an alert. Value range is 50% to 85%.
-FASTCacheEnabled	Specify whether to enable FAST Cache on the storage pool. Value is one of the following: • Yes • No Default value is Yes.
-snapPoolFullThresholdEnabled	Indicate whether the system should check the pool full high water mark for auto-delete. Value is one of the following: • Yes • No Default value is Yes.
-snapPoolFullHWM	Specify the pool full high watermark for the storage pool. Valid values are 1-99. Default value is 95.
-snapPoolFullLWM	Specify the pool full low watermark for the storage pool. Valid values are 0-98. Default value is 85.
-snapSpaceUsedThresholdEnabled	Indicate whether the system should check the snapshot space used high water mark for auto-delete. Value is one of the following: • Yes • No Default value is Yes.
-snapSpaceUsedHWM	Specify the snapshot space used high watermark to trigger auto-delete on the storage pool. Valid values are 1-99. Default value is 95.
-snapSpaceUsedLWM	Specify the snapshot space used low watermark to trigger auto-delete on the storage pool. Valid values are 0-98. Default value is 20.

Example 1 (physical deployments only)

The following command creates a storage pool that uses storage profiles SP_1and SP_2, and seven disks from disk group DG_1 and five disks from disk group DG_2. The configured storage pool receives ID SPL_4:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool
create -name GlobalPool1 –descr "Oracle databases" –storProfile SP_1
SP_2 –diskGroup DG_1 DG_2 –drivesNumber 7 5
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = SPL_4
Operation completed successfully.
```

Example 2 (virtual deployments only)

The following command creates a storage pool with two virtual disks, vdisk_0 and vdisk_2 in the extreme tier. The configured storage pool receives ID pool_4.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool
create -name vPool -descr "my virtual pool" -disk vdisk_0,vdisk_2 -
tier extreme
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = pool_4
Operation completed successfully.
```

View storage pools

View a list of storage pools. You can filter on the storage pool ID.

Note

explains how to change the output format.

Format
```
/stor/config/pool [-id <value>] show
```

Object qualifier

Qualifier	Description
-id	Type the ID of a storage pool.

Example 1 (physical deployments only)

The following command shows details about all storage pools on the system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool
show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: ID                                                  = SPL_1
   Name                                                = Performance
   Description                                         = Multi-tier pool
```

```
   Total space                                   = 4947802324992
(4.5T)
   Current allocation                            = 3298534883328
(3T)
   Remaining space                               = 1649267441664
(1.5T)
   Subscription                                  = 10995116277760
(10T)
   Subscription percent                          = 222%
   Alert threshold                               = 70%
   Drives                                        = 6 x 100GB EFD;
6 x 300GB SAS
   Number of drives                              = 12
   RAID level                                    = Mixed
   Stripe length                                 = Mixed
   Rebalancing                                   = no
   Rebalancing progress                          =
   Health state                                  = OK (5)
   Health details                                = "The component
is operating normally.  No action is required."
   FAST Cache enabled                            = no
   Protection size used                          = 1099511625 (1G)
   Auto-delete state                             = Running
   Auto-delete paused                            = no
   Auto-delete pool full threshold enabled       = yes
   Auto-delete pool full high water mark         = 95%
   Auto-delete pool full low water mark          = 85%
   Auto-delete snapshot space used threshold enabled = yes
   Auto-delete snapshot space used high water mark   = 25%
   Auto-delete snapshot space used low water mark    = 20%


2: ID                                            = SPL_2
   Name                                          = Capacity
   Description                                   =
   Total space                                   = 4947802324992
(4.5T)
   Current allocation                            = 3298534883328
(3T)
   Remaining space                               = 1649267441664
(1.5T)
   Subscription                                  = 10995116277760
(10T)
   Subscription percent                          = 222%
   Alert threshold                               = 70%
   Drives                                        = 12 x 2TB NL-SAS
   Number of drives                              = 12
   Unused drives                                 = 7
   RAID level                                    = 6
   Stripe length                                 = 6
   Rebalancing                                   = yes
   Rebalancing progress                          = 46%
   Health state                                  = OK (5)
   Health details                                = "The component
is operating normally.  No action is required."
   FAST Cache enabled                            = yes
   Protection size used                          = 10995116238
(10G)
   Auto-delete state                             = Running
   Auto-delete paused                            = no
   Auto-delete pool full threshold enabled       = yes
   Auto-delete pool full high water mark         = 95%
   Auto-delete pool full low water mark          = 85%
   Auto-delete snapshot space used threshold enabled = yes
   Auto-delete snapshot space used high water mark   = 25%
   Auto-delete snapshot space used low water mark    = 20%
```

Example 2 (virtual deployments only)

The following command shows details for all storage pools on a virtual system.

uemcli -d 10.0.0.2 -u Local/joe -p MyPassword456! /stor/config/pool show -detail

```
Storage system address: 10.0.0.2
Storage system port: 443
HTTPS connection

1:     ID                                              = pool_1
       Name                                            = Capacity
       Description                                     =
       Total space                                     =
4947802324992 (4.5T)
       Current allocation                              =
3298534883328 (3T)
       Remaining space                                 =
4947802324992 (1.5T)
       Subscription                                    =
10995116277760 (10T)
       Subscription percent                            = 222%
       Alert threshold                                 = 70%
       Drives                                          = 1 x 120GB
Virtual; 1 x 300GB Virtual
       Number of drives                                = 2
       Health state                                    = OK (5)
       Health details                                  = "The
component is operating normally.  No action is required."
       Protection size used                            = 1099511625
(1G)
       Auto-delete state                               = Running
       Auto-delete paused                              = no
       Auto-delete pool full threshold enabled         = yes
       Auto-delete pool full high water mark           = 95%
       Auto-delete pool full low water mark            = 85%
       Auto-delete snapshot space used threshold enabled = yes
       Auto-delete snapshot space used high water mark = 25%
       Auto-delete snapshot space used low water mark  = 20%
```

Change storage pool settings

Change the subscription alert threshold setting for a storage pool.

Format

```
/stor/config/pool -id <value> set [-async] -name <value> [-
descr <value>] [-alertThreshold <value>] [-
snapPoolFullThresholdEnabled {yes|no}] [-snapPoolFullHWM
<value>] [-snapPoolFullLWM <value>] [-
snapSpaceUsedThresholdEnabled {yes|no}] [-snapSpaceUsedHWM
<value>] [-snapSpaceUsedLWM <value>]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the storage pool to change.

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.

Qualifier	Description
-name	Type a name for the storage pool.
-descr	Type a brief description of the storage pool.
-alertThreshold	For thin provisioning, specify the threshold, as a percentage, when the system will alert on the amount of subscription space used. When hosts consume the specified percentage of subscription space, the system sends an alert. Value range is 50% to 85%.
-FASTCacheEnabled	Specify whether to enable FAST Cache on the storage pool. Value is one of the following: • Yes • No Default value is Yes.
-snapPoolFullThresholdEnabled	Indicate whether the system should check the pool full high water mark for auto-delete. Value is one of the following: • Yes • No Default value is Yes.
-snapPoolFullHWM	Specify the pool full high watermark for the storage pool. Valid values are 1-99. Default value is 95.
-snapPoolFullLWM	Specify the pool full low watermark for the storage pool. Valid values are 0-98. Default value is 85.
-snapSpaceUsedThresholdEnabled	Indicate whether the system should check the snapshot space used high water mark for auto-delete. Value is one of the following: • Yes • No Default value is Yes.
-snapSpaceUsedHWM	Specify the snapshot space used high watermark to trigger auto-delete on the storage pool. Valid values are 1-99. Default value is 95.
-snapSpaceUsedLWM	Specify the snapshot space used low watermark to trigger auto-delete on the storage pool. Valid values are 0-98. Default value is 20.

Qualifier	Description
-snapAutoDeletePaused	Specify whether to pause snapshot auto-delete. Typing `no` resumes the auto-delete operation.

Example

The following command sets the subscription alert threshold for storage pool SPL_1 to 70%:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool -
id SPL_1 -set -alertThreshold 70 -FASTCacheEnabled no
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = SPL_1
Operation completed successfully.
```

Add disks or tiers to storage pools

Add new disks to a storage pool to increase its storage capacity.

Format

```
/stor/config/pool -id <value> extend [-async] {-diskGroup
<value> -drivesNumber <value> [-storProfile <value>] |-disk
<value> [-tier <value>]}
```

Object qualifier

Qualifier	Description
-id	Type the ID of the storage pool to extend.

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.
-diskGroup (physical deployments only)	Type the IDs of the disk groups, separated by commas, to add to the storage pool.
-drivesNumber (physical deployments only)	Type the number of disks from the specified disk groups, separated by commas, to add to the storage pool. If this option is specified when -storProfile is not specified, the operation may fail when the -drivesNumber value does not match the default RAID configuration for each drive type in the selected disk group.
-storProfile (physical deployments only)	Type the IDs of the storage profiles, separated by commas, to apply to the storage pool. If this option is not specified, a default RAID configuration is selected for each particular drive type in the selected disk group: NL-SAS (RAID 6 with a stripe length of 8), SAS (RAID 5 with a stripe length of 5), or Flash (RAID 5 with a stripe length of 5).

Qualifier	Description
-disk (virtual deployments only)	Specify the list of disks, separated by commas, to add to the storage pool. Specified disks must be reliable storage objects which do not require additional protection.
-tier (virtual deployments only)	Specify the list of tiers, separated by commas, to which the disks are assigned. If a tier is omitted, it will be assigned automatically if tiering information for associated disk is available. Valid values include: • capacity • performance • extreme

Example 1 (physical deployments only)

The following command extends storage pool SPL_1 with seven disks from disk group DG_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool -
id SPL_1 extend -diskGroup DG_1 -drivesNumber 7 -storProfile
profile_12
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = SPL_1
Operation completed successfully.
```

Example 2 (virtual deployments only)

The following command extends storage pool pool_1 by adding two virtual disks, vdisk_1 and vdisk_5.

```
uemcli -d 10.0.0.2 -u Local/joe -p MyPassword456! /stor/config/pool -
id pool_1 extend -disk vdisk_1,vdisk_5
```

```
Storage system address: 10.0.0.2
Storage system port: 443
HTTPS connection

ID = pool_1
Operation completed successfully.
```

Delete storage pools

Delete a storage pool.

Format
```
/stor/config/pool -id <value> delete [-async]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the storage pool to extend.

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.

Example

The following deletes storage pool SPL_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool –id SPL_1 delete

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage storage pool tiers

Storage tiers allow users to move data between different types of disks in a storage pool to maximize storage efficiency. Storage tiers are defined by the following characteristics:

- Disk performance.
- Disk capacity.

The following table lists the attributes for storage profiles:

Table 67 Storage tier attributes

Attribute	Description
Name	Storage tier name.
Drives	The list of disk types, and the number of disks of each type in the storage tier.
RAID level (physical deployments only)	RAID level of the storage tier.
Stripe length (physical deployments only)	Comma-separated list of the stripe length of the disks in the storage tier.
Total space	Total capacity in the storage tier.
Current allocation	Currently allocated space.
Remaining space	Remaining space.

View storage tiers

View a list of storage tiers. You can filter on the storage pool ID.

Note

The show action command on page 17 explains how to change the output format.

Format
```
/stor/config/pool/tier –pool <value> show
```

Object qualifier

Qualifier	Description
`-pool`	Type the ID of a storage pool.

Example 1 (physical deployments only)

The following command shows details about all storage pools on the system:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool/`
`tier -pool SPL_1 show -detail`

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      Name                = Extreme Performance
        Drives              =
        RAID level          =
        Stripe length       =
        Total space         = 0
        Current allocation  = 0
        Remaining space     = 0


2:      Name                = Performance
        Drives              = 5 x 300GB SAS
        RAID level          = 5
        Stripe length       = 5
        Total space         = 928180076544 (864.4G)
        Current allocation  = 8606711808 (8.0G)
        Remaining space     = 919573364736 (856.4G)


3:      Name                = Capacity
        Drives              =
        RAID level          =
        Stripe length       =
        Total space         = 0
        Current allocation  = 0
        Remaining space     = 0
```

Example 2 (virtual deployments only)

The following command shows details about storage pool pool_1 on a virtual system.

`uemcli -d 10.0.0.2 -u Local/joe -p MyPassword456! /stor/config/pool/`
`tier –pool pool_1 show -detail`

```
Storage system address: 10.0.0.2
Storage system port: 443
HTTPS connection

1:      Name                = Extreme Performance
        Drives              =
        Total space         = 0
        Current allocation  = 0
        Remaining space     = 0


2:      Name                = Performance
        Drives              = 1 x 500GB Virtual
        Total space         = 631242752000 (500.0G)
        Current allocation  = 12624855040 (10.0G)
        Remaining space     = 618617896960 (490.0G)
```

```
3:      Name                = Capacity
        Drives              =
        Total space         = 0
        Current allocation  = 0
        Remaining space     = 0
```

Manage FAST VP pool settings

Fully Automated Storage Tiering for Virtual Pools (FAST VP) is a storage efficiency technology that automatically moves data between storage tiers within a storage pool based on data access patterns.

The following table lists the attributes for FAST VP pool settings.

Table 68 FAST VP pool attributes

Attribute	Description
Pool	Identifies the storage pool.
Status	Identifies the status of data relocation on the storage pool. Value is one of the following: • `Not started` - Data relocation has not started. • `Paused` - Data relocation is paused. • `Completed` - Data relocation is complete. • `Stopped by user` - Data relocation was stopped by the user. • `Active` - Data relocation is in progress. • `Failed` - Data relocation failed.
Relocation type	Type of data relocation. Value is one of the following: • `Manual` - Data relocation was initiated by the user. • `Scheduled` or `rebalancing` - Data relocation was initiated by the system because it was scheduled, or because the system rebalanced the data.
Schedule enabled	Identifies whether the pool is rebalanced according to the system FAST VP schedule. Value is one of the following: • `Yes` • `No`
Start time	Indicates the time the current data relocation started.
End time	Indicates the time the current data relocation is scheduled to end.
Data relocated	The amount of data relocated during an ongoing relocation, or the previous relocation if a data relocation is not occurring. The format is: `<value>[suffix]` where: • *value* - Identifies the size of the data relocated.

Table 68 FAST VP pool attributes (continued)

Attribute	Description
	• *suffix* - Identifies that the value relates to the previous relocation session.
Rate	Identifies the transfer rate for the data relocation. Value is one of the following: • `Low` - Least impact on system performance. • `Medium` - Moderate impact on system performance. • `High` - Most impact on system performance. Default value is medium. **Note** This field is blank if data relocation is not in progress.
Data to move up	The amount of data in the storage pool scheduled to be moved to a higher storage tier.
Data to move down	The amount of data in the storage pool scheduled to be moved to a lower storage tier.
Data to move within	The amount of data in the storage pool scheduled to be moved within the same storage tiers for rebalancing.
Data to move up per tier	The amount of data per tier that is scheduled to be moved to a higher tier. The format is: `<tier_name>`:`[value]` where: • *tier_name* - Identifies the storage tier. • *value* - Identifies the amount of data in that tier to be move up.
Data to move down per tier	The amount of data per tier that is scheduled to be moved to a lower tier. The format is: `<tier_name>`:`[value]` where: • *tier_name* - Identifies the storage tier. • *value* - Identifies the amount of data in that tier to be moved down.
Data to move within per tier	The amount of data per tier that is scheduled to be moved to within the same tier for rebalancing. The format is: `<tier_name>`:`[value]` where: • *tier_name* - Identifies the storage tier. • *value* - Identifies the amount of data in that tier to be rebalanced.

Table 68 FAST VP pool attributes (continued)

Attribute	Description
Estimated relocation time	Identifies the estimated time required to perform the next data relocation.

Change FAST VP pool settings

Modify FAST VP settings on an existing pool.

Format
```
/stor/config/pool/fastvp -pool <value> set [-async] -
schedEnabled {yes | no}
```

Object qualifier

Qualifier	Description
-pool	Type the ID of the storage pool.

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.
-schedEnabled	Specify whether the pool is rebalanced according to the system FAST VP schedule. Value is one of the following: • Yes • No

Example
The following example enables the rebalancing schedule on storage pool pool_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool/
fastvp -pool pool_1 set -schedEnabled yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Pool ID = pool_1
Operation completed successfully.
```

View FAST VP pool settings

View FAST VP settings on a storage pool.

Format
```
/stor/config/pool/fastvp [-pool <value>] show
```

Object qualifier

Qualifier	Description
-pool	Type the ID of the storage pool.

Example

The following command lists the FAST VP settings on the storage system:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool/
fastvp -show -detail

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: Pool                       = pool_1
   Relocation type            = manual
   Status                     = Active
   Schedule enabled           = no
   Start time                 = 2013-09-20 12:55:32
   End time                   = 2013-09-20 21:10:17
   Data relocated             = 100111454324 (100G)
   Rate                       = high
   Data to move up            = 4947802324992 (4.9T)
   Data to move down          = 4947802324992 (4.9T)
   Data to move within        = 4947802324992 (4.9T)
   Data to move up per tier   = Performance: 500182324992 (500G),
Capacity:    1000114543245 (1.0T)
   Data to move down per tier    = Extreme Performance: 1000114543245
(1.0T),    Performance: 500182324992 (500G)
   Data to move within per tier  = Extreme Performance: 500182324992
(500G),    Performance: 500182324992 (500G), Capacity: 500182324992
(500G)
   Estimated relocation time     = 7h 30m
```

Start data relocation

Start data relocation on a storage pool.

Format
```
/stor/config/pool/fastvp -pool <value> start [-async] [-rate
{low | medium | high}] [-endTime <value>]
```

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.
-pool	Type the ID of the storage pool.
-endTime	Specify the time to stop the data relocation. The format is: `[HH:MM]` where: • HH — Hour. • MM — Minute. Default value is eight hours from the current time.

Qualifier	Description
-rate	Specify the transfer rate for the data relocation. Value is one of the following: • `Low` — Least impact on system performance. • `Medium` — Moderate impact on system performance. • `High` — Most impact on system performance. Default value is the value set at the system level.

Example

The following command starts data relocation on storage pool pool_1, and directs it to end at 04:00:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool/
fastvp -pool pool_1 start -endTime 04:00

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Stop data relocation

Stop data relocation on a storage pool.

Format
/stor/config/pool/fastvp –pool <value> stop [-async]

Object qualifier

Qualifier	Description
-pool	Type the ID of the storage pool.

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.

Example

The following command stops data relocation on storage pool pool_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool/
fastvp –pool pool_1 stop

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

View storage pool resources

This command displays a list of storage resources allocated in a storage pool. This can be storage resources provisioned on specified storage pool, and NAS servers that have file systems allocated in the pool.

The following table lists the attributes for storage pool resources.

Table 69 Storage pool resources

Attribute	Description
ID	Storage resource identifier.
Name	Name of the storage resource.
Resource type	Type of the resource. Valid values are LUN, File system, LUN group, VMware NFS, VMware VMFS, and NAS server.
Pool	Name of the storage pool.
Total pool space used	Total space used by the storage pool. This includes primary data used size, snapshot used size, and metadata size.
Total pool snapshot space used	Total spaced used by the storage pool for snapshots.
Health state	Health state of the file system. The health state code appears in parentheses.
Health details	Additional health information. See Appendix A, Reference, for health information details.

Note

The show action command on page 17 explains how to change the output format.

Format
```
/stor/config/pool/sr [-pool <value>] show
```

Object qualifier

Qualifier	Description
-pool	Type the name of the storage pool.

Example
The following command shows details for all storage resources associated with the storage pool pool_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool/sr -pool pool_1 show -detail

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1:      ID                          = res_1
        Name                        = FileSystem00
        Resource type               = File system
        Pool                        = pool_1
        Total pool space used       = 23622320128 (220GB)
        Total pool snapshot space used = 2147483648 (2GB)
        Health state                = OK (5)
        Health details              = "The component is operating
normally. No action is required."

2:      ID                          = res_2
        Name                        = LUNGroup00
        Resource type               = LUN group
        Pool                        = pool_1
        Total pool space used       = 57982058496 (54GB)
        Total pool snapshot space used = 4294967296 (4GB)
        Health state                = OK (5)
        Health details              = "The component is operating
normally. No action is required."

3:      ID                          = nas_1
        Name                        = NASServer00
        Resource type               = NAS server
        Pool                        = pool_1
        Total pool space used       =
        Total pool snapshot space used =
        Health state                = OK (5)
        Health details              = "The component is operating
normally. No action is required."
```

Manage FAST VP general settings

Fully Automated Storage Tiering for Virtual Pools (FAST VP) is a storage efficiency technology that automatically moves data between storage tiers within a storage pool based on data access patterns.

The following table lists the attributes for FAST VP general settings.

Table 70 FAST VP general attributes

Attribute	Description
Paused	Identifies whether the data relocation is paused. Value is one of the following: ● Yes ● No
Schedule-enabled	Identifies whether the pool is rebalanced according to the system FAST VP schedule. Value is one of the following: ● Yes ● No
Frequency	Data relocation schedule. The format is: Every *<days_of_the_week>* at *<start_time>* until *<end_time>* where: ● *<days_of_the_week>* - List of the days of the week that data relocation will run. ● *<start_time>* - Time the data relocation starts. ● *<end_time>* - Time the data relocation finishes.

Table 70 FAST VP general attributes (continued)

Attribute	Description
Rate	Identifies the transfer rate for the data relocation. Value is one of the following: • Low - Least impact on system performance. • Medium - Moderate impact on system performance. • High - Most impact on system performance. Default value is medium. **Note** This field is blank if data relocation is not in progress.
Data to move up	The amount of data in the storage pool scheduled to be moved to a higher storage tier.
Data to move down	The amount of data in the storage pool scheduled to be moved to a lower storage tier.
Data to move within	The amount of data in the storage pool scheduled to be moved within the same storage tiers for rebalancing.
Estimated relocation time	Identifies the estimated time required to perform the next data relocation.

Change FAST VP general settings

Change FAST VP general settings.

Format
```
/stor/config/fastvp set [-async] [-schedEnabled {yes | no}] [-
days <value>] [-at <value>] [-until <value>] [-rate {low |
medium | high}] [-paused {yes | no}]
```

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.
-paused	Specify whether to pause data relocation on the storage system. Value is one of the following: • Yes • No
-schedEnabled	Specify whether the pool is rebalanced according to the system FAST VP schedule. Value is one of the following: • Yes • No

Qualifier	Description
-days	Specify a comma-separated list of the days of the week to schedule data relocation. Valid values are: • Mon – Monday • Tue – Tuesday • Wed – Wednesday • Thu – Thursday • Fri – Friday • Sat – Saturday • Sun – Sunday
-at	Specify the time to start the data relocation. The format is: `[HH:MM]` where: • HH – Hour • MM – Minute Valid values are between `00:00` and `23:59`. Default value is `00:00`.
-until	Specify the time to stop the data relocation. The format is: `[HH:MM]` where: • HH – Hour • MM – Minute Valid values are between `00:00` and `23:59`. Default value is eight hours after the time specified with the -at parameter.
-rate	Specify the transfer rate for the data relocation. Value is one of the following: • Low – Least impact on system performance. • Medium – Moderate impact on system performance. • High – Most impact on system performance. Default value is medium.

Example

The following command changes the data relocation schedule to run on Mondays and Fridays from 23:00 to 07:00:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/fastvp
set -schedEnabled yes -days "Mon,Fri" -at 23:00 -until 07:00
```

```
Storage system address: 10.0.0.1
Storage system port: 443
```

```
HTTPS connection

Operation completed successfully.
```

View FAST VP general settings

View the FAST VP general settings.

Format
`/stor/config/fastvp show -detail`

Example
The following command displays the FAST VP general settings:

**uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/fastvp
show -detail**

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: Paused                            = no
   Schedule enabled                  = yes
   Frequency                         = Every Mon, Fri at 22:30
until 8:00
   Rate                              = high
   Data to move up                   = 4947802324992 (1.5T)
   Data to move down                 = 4947802324992 (1.5T)
   Data to move within               = 4947802324992 (1.5T)
   Estimated scheduled relocation time = 7h 30m
```

Manage FAST Cache (physical deployments only)

FAST Cache is a storage efficiency technology that uses disks to expand the cache
capability of the storage system to provide improved performance.

The following table lists the attributes for FAST Cache:

Table 71 FAST Cache attributes

Attribute	Description
Capacity	Capacity of the FAST Cache.
Drives	The list of disk types, and the number of disks of each type in the FAST Cache.
Number of drives	Total number of disks in the FAST Cache.
RAID level	RAID level applied to the FAST Cache disks. This value is always **RAID 1**.
Health state	Health state of the FAST Cache. The health state code appears in parentheses.
Health details	Additional health information. See Appendix A, Reference, for health information details.

Create FAST Cache

Configure FAST Cache. The storage system generates an error if FAST Cache is already configured.

Format
```
/stor/config/fastcache create [-async] -diskGroup <value> -
drivesNumber <value> [-enableOnExistingPools]
```

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.
-diskGroup	Specify the disk group to include in the FAST Cache.
-drivesNumber	Specify the number of disks to include in the FAST Cache.
-enableOnExistingPools	Specify whether FAST Cache is enabled on all existing pools.

Example
The following command configures FAST Cache with six disks from disk group DG_1, and enables FAST Cache on existing storage pools:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/
fastcache create -diskGroup DG_1 -drivesNumber 6 -
enableOnExistingPools

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

View FAST Cache settings

View the FAST Cache parameters.

Format
```
/stor/config/fastcache show
```

Example
The following command displays the FAST Cache parameters:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/
fasdtcache show -detail

```
1:     Total space      = 536870912000 (500G)
       Drives           = 6 x 100GB SAS Flash
       Number of drives = 6
       RAID level       = 1
       Health state     = OK (5)
       Health details   = "The component is operating normally. No
action is required."
```

Delete FAST Cache

Delete the FAST Cache configuration. The storage system generates an error if FAST Cache is not configured on the system.

Format
```
/stor/config/fastcache delete [-async]
```

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.

Example
The following command deletes the FAST Cache configuration:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/
fastcache delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

View storage profiles (physical deployments only)

Storage profiles are preconfigured settings for configuring storage pools based on the following:

- Types of storage resources that will use the pools.
- Intended usage of the pool.

For example, create a storage pool for file system storage resources intended for general use. When configuring a storage pool, specify the ID of the storage profile to apply to the pool.

Note

Storage profiles are not restrictive with regard to storage provisioning. For example, you can provision file systems from an FC or iSCSI database storage pool. However, the characteristics of the storage will be best suited to the indicated storage resource type and use.

Each storage profile is identified by an ID.

The following table lists the attributes for storage profiles.

Table 72 Storage profile attributes

Attribute	Description
ID	ID of the storage profile.
Description	Brief description of the storage profile.
Drive type	Types of disks for the storage profile.

Table 72 Storage profile attributes (continued)

Attribute	Description
RAID level	RAID level number for the storage profile. Value is one of the following: • `1` - RAID level 1. • `5` - RAID level 5. • `6` - RAID level 6. • `10` – RAID level 1+0.
Maximum capacity	Maximum storage capacity for the storage profile.
Stripe length	Number of disks the data is striped across. **Note** For best fit profiles, this value is `Best fit`.

Note

explains how to change the output format.

Format

```
/stor/config/profile [-id <value> | -driveType <value> [-
raidLevel <value>]] show
```

Object qualifier

Qualifier	Description
-id	Type the ID of a storage profile.
-driveType	Specify the type of disk drive.
-raidLevel	Specify the RAID type of the profile.

Example

The following command shows details for all storage profiles on the system:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/profile show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:     ID               = SP_1
       Description      = Best Performance
       Drive type       = SAS
       RAID level       = 5
       Maximum capacity = 1099511627776 (1TB)
       Stripe length    = 6

2:     ID               = SP_2
       Description      = High Capacity
       Drive type       = FAT-SAS
       RAID level       = 6
       Maximum capacity = 21990232555520 (20TB)
```

```
        Stripe length    = 6

3:      ID               = SP_3
        Name             = Performance
        Drive type       = SAS
        RAID level       = 5
        Maximum capacity = 5937362789990 (5.4TB)
        Stripe length    = 5
```

Manage disk groups (physical deployments only)

Disk groups are the groups of disks on the system with similar characteristics, including type, capacity, and spindle speed. When configuring storage pools, you select the disk group to use and the number of disks from the group to add to the pool.

Each disk group is identified by an ID.

The following table lists the attributes for disk groups.

Table 73 Disk group attributes

Attribute	Description
ID	ID of the disk group.
Drive type	Type of disks in the disk group.
Drive size	Capacity of one disk in the disk group.
Rotational speed	Rotational speed of the disks in the group.
Number of drives	Total number of disks in the disk group.
Unconfigured drives	Total number of disks in the disk group that are not in a storage pool.
Capacity	Total capacity of all disks in the disk group.
Recommended number of spares	Number of spares recommended for the disk group.

View disk groups

View details about disk groups on the system. You can filter on the disk group ID.

Note

explains how to change the output format.

Format
/stor/config/dg [-id <value>] show

Object qualifier

Qualifier	Description
-id	Type the ID of a disk group.

Example
The following command shows details about all disk groups:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/dg show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: ID                          = DG_1
   Drive type                  = FAT-SAS
   Drive size                  = 536870912000 (500GB)
   Rotational speed            = 10000 rpm
   Number of drives            = 21
   Unconfigured drives         = 7
   Capacity                    = 11544872091648 (10.5TB)
   Recommended number of spares = 1

2: ID                          = DG_2
   Drive type                  = FAT-SAS
   Drive size                  = 1099511627776 (1TB)
   Rotational speed            = 7200 rpm
   Number of drives            = 14
   Unconfigured drives         = 0
   Capacity                    = 15393162788864 (14TB)
   Recommended number of spares = 1

3: ID                          = DG_3
   Drive type                  = SAS
   Drive size                  = 107374182400 (100GB)
   Rotational speed                        = 10000 rpm
   Number of drives            = 10
   Unconfigured drives         = 3
   Capacity                    = 1099511627776 (1TB)
   Recommended number of spares = 1
```

View recommended disk group configurations

View the recommended disk groups from which to add disks to a storage pool based on a specified storage profile or pool type.

Note

The show action command on page 17 explains how to change the output format.

Format
/stor/config/dg recom {-profile <value>|-pool <value>}

Action qualifier

Qualifier	Description
-profile	Type the ID of a storage profile. The output will include the list of disk groups recommended for the specified storage profile.
-pool	Type the ID of a storage pool. The output will include the list of disk groups recommended for the specified storage pool.

Example
The following command shows the recommended disk groups for storage pool SPL_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/dg
recom -pool SPL_1
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1:      ID                    = DG_1
        Drive type            = SAS
        Drive size            = 536870912000 (500GB)
        Number of drives      = 8
        Allowed numbers of drives = 4,8
        Capacity              = 4398046511104 (4TB)

2:      ID                    = DG_2
        Drive type            = SAS
        Drive size            = 268435456000 (250GB)
        Number of drives      = 4
        Allowed numbers of drives = 4
        Capacity              = 1099511627776 (1TB)
```

Manage file systems

File systems are logical containers on the system that provide file-based storage resources to hosts. You configure file systems on NAS servers, which maintain and manage the file systems. You create network shares on the file system, which connected hosts map or mount to access the file system storage. When creating a file system, you can enable support for the following network shares:

- Common Internet File System (CIFS) shares, which provide storage access to Windows hosts.

- Network file system (NFS) shares, which provide storage access to Linux/UNIX hosts.

Each file system is identified by an ID.

The following table lists the attributes for file systems:

Table 74 File system attributes

Attribute	Description
ID	ID of the file system.
Name	Name of the file system.
Description	Description of the file system.

Health state	Health state of the file system. The health state code appears in parentheses. Value is one of the following:
	
	• OK (5) - File system is operating normally.
	
	• Degraded/Warning (10) - Working, but one or more of the following may have occurred:
	
	  ■ One or more of its storage pools are degraded.
	
	  ■ It has almost reached full capacity. Increase the primary storage size, or create additional file systems to store your data, to avoid data loss. Change file system settings on page 224 explains how to change the primary storage size.
	
	• Minor failure (15) - One or both of the following may have occurred:
	
	  ■ One or more of its storage pools have failed.
	
	  ■ The associated NAS server has failed.

Table 74 File system attributes (continued)

Attribute	Description
	• `Major failure (20)` - One or both of the following may have occurred: ■ One or more of its storage pools have failed. ■ File system is unavailable. • `Critical failure (25)` - One or more of the following may have occurred: ■ One or more of its storage pools are unavailable. ■ File system is unavailable. ■ File system has reached full capacity. Increase the primary storage size, or create additional file systems to store your data, to avoid data loss. Change file system settings on page 224 explains how to change the primary storage size. • `Non-recoverable error (30)` - One or both of the following may have occurred: ■ One or more of its storage pools are unavailable. ■ File system is unavailable.
`Health details`	Additional health information. See Appendix A, Reference, for health information details.
`File system`	Identifier for the file system. Output of some metrics commands display only the file system ID. This will enable you to easily identify the file system in the output.
`Server name`	Name of the primary NAS server that the file system uses.
`Storage pool ID`	ID of the storage pool the file system is using.
`Storage pool`	Name of the storage pool that the file system uses.
`Protocol`	Protocol used to enable network shares from the file system. Values are one of the following: • `nfs` - Protocol for Linux/UNIX hosts. • `cifs` - Protocol for Windows hosts. • `multiprotocol` - Protocol for UNIX and Windows hosts.
`Access policy`	Access policy type for this file system. Values are one of the following: • `native` (default) - When this policy is selected, Unix mode bits are used for Unix/Linux clients, and Windows permissions (ACLs) are used for Windows clients. • `Unix` - When this policy is selected, Unix mode bits are used to grant access to each file on the file system. • `Windows` - When this policy is selected, permissions defined in Windows ACLs are honored for both Windows and Unix/Linux clients (Unix mode bits are ignored).

Table 74 File system attributes (continued)

Attribute	Description
Size	Quantity of storage reserved for primary data.
Size used	Quantity of storage currently used for primary data.
Maximum size	Maximum size to which you can increase the primary storage capacity.
Thin provisioning enabled	Indication of whether thin provisioning is enabled. Value is yes or no. Default is no. All storage pools support both standard and thin provisioned storage resources. For standard storage resources, the entire requested size is allocated from the pool when the resource is created, for thin provisioned storage resources only incremental portions of the size are allocated based on usage. Because thin provisioned storage resources can subscribe to more storage than is actually allocated to them, storage pools can be over provisioned to support more storage capacity than they actually possess. **Note** The Unisphere online help provides more details on thin provisioning.
Current allocation	If enabled, the quantity of primary storage currently allocated through thin provisioning.
Protection size used	Quantity of storage currently used for protection data.
Protection schedule	ID of an applied protection schedule. View protection schedules on page 55 explains how to view the IDs of schedules on the system.
Protection schedule paused	Indication of whether an applied protection schedule is currently paused. Value is yes or no.
FAST VP policy	FAST VP policy of the file system. Value is one of the following: • Start high then auto-tier • Auto-tier • Highest available tier • Lowest available tier
FAST VP distribution	Percentage of the file system storage assigned to each tier. The format is: `<tier_name>:<value>%` where, *‹tier_name›* is the name of the storage tier and *‹value›* is the percentage of storage in that tier.
File level retention	Indication of whether file-level retention (FLR) is enabled. Value is yes or no. FLR provides a way to set file-based permissions to limit write access to the files for a specific period of time. In this way, file-level retention can ensure the integrity of data during that period by creating an unalterable set of files and directories.

Table 74 File system attributes (continued)

Attribute	Description
	Note
	File-level retention prevents files from being modified or deleted by NAS clients and users. Once you enable FLR for a Windows file system, you cannot disable it. Leave FLR disabled unless you intend to implement self-regulated archiving and you intend the administrator to be the only trusted user of the file system on which FLR is enabled. The Unisphere online help and the host documentation provide more details on FLR.
CIFS synchronous write	Indication of whether CIFS synchronous writes option is enabled. Value is `yes` or `no`.
	• The CIFS synchronous writes option provides enhanced support for applications that store and access database files on Windows network shares. On most CIFS filesystems read operations are synchronous and write operations are asynchronous. When you enable the CIFS synchronous writes option for a Windows (CIFS) file system, the system performs immediate synchronous writes for storage operations, regardless of how the CIFS protocol performs write operations.
	• Enabling synchronous write operations allows you to store and access database files (for example, MySQL) on CIFS network shares. This option guarantees that any write to the share is done synchronously and reduces the chances of data loss or file corruption in various failure scenarios, for example, loss of power.
	Note
	Do not enable CIFS synchronous writes unless you intend to use the Windows file systems to provide storage for database applications.
	The Unisphere online help provides more details on CIFS synchronous write.
CIFS oplocks	Indication of whether opportunistic file locks (oplocks) for CIFS network shares are enabled. Value is `yes` or `no`.
	• Oplocks allow CIFS clients to buffer file data locally before sending it to a server. CIFS clients can then work with files locally and periodically communicate changes to the system, rather than having to communicate every operation to the system over the network.
	• This feature is enabled by default for Windows (CIFS) file systems. Unless your application handles critical data or has specific requirements that make this mode or operation unfeasible, leave oplocks enabled.
	The Unisphere online help provides more details on CIFS oplocks.
CIFS notify on write	Indication of whether write notifications for CIFS network shares are enabled. Value is yes or no. When enabled, Windows applications receive notifications each time a user writes or changes a file on the CIFS share.

Table 74 File system attributes (continued)

Attribute	Description
	Note If this option is enabled, the value for CIFS directory depth indicates the lowest directory level to which the notification setting applies.
CIFS notify on access	Indication of whether file access notifications for CIFS shares are enabled. Value is yes or no. When enabled, Windows applications receive notifications each time a user accesses a file on the CIFS share. **Note** If this option is enabled, the value for CIFS directory depth indicates the lowest directory level to which the notification setting applies.
CIFS directory depth	For write and access notifications on CIFS network shares, the subdirectory depth permitted for file notifications. Value range is 1-512. Default is 512.
Deduplication enabled	Indication of whether deduplication is enabled on the file system. Value is: • Yes • No
Creation time	Date and time when the file system was created.
Last modified time	Date and time when the file system settings were last changed.
Snapshot count	Number of snapshots created on the file system.

Create file systems

Create an NFS file system or CIFS file system. You must create a file system for each type of share (NFS or CIFS) you plan to create. Once you create a file system, create the NFS or CIFS network shares and use the ID of file system to associate it with a share.

Note

Size qualifiers on page 16 provides details on using size qualifiers to specify a storage size.

Prerequisites

- Configure at least one storage pool for the file system to use and allocate at least one storage disk to the pool. Configure storage pools automatically (physical deployments only) on page 186 explains how to create pools on the system automatically and Configure custom storage pools on page 188 explains how to create custom pools.

- Configure at least one NAS server to which to associate the file system. Create NAS servers on page 72 explains how to configure NAS servers.

Format

```
/stor/prov/fs create [-async] -name <value> [-descr <value>] -
server <value> -pool <value> -size <value> [-thin {yes | no}] -
type {cifs | multiprotocol}[-cifsSyncWrites {yes | no}] [-
cifsOpLocks {yes | no}] [-cifsNotifyOnWrite {yes | no}] [-
cifsNotifyOnAccess {yes | no}] [-cifsNotifyDirDepth <value>] |
nfs} [-accessPolicy {native | Windows | Unix}] [-fastvpPolicy
{ startHighThenAuto | auto | highest | lowest}] [-fileLevelRet
{yes | no}] [-sched <value> [-schedPaused {yes | no}]]
```

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.
-name	Type a name for the file system.
-descr	Type a brief description of the file system.
-server	Type the ID of the NAS server that will be the primary NAS server for the file system. View NAS servers on page 74 explains how to view the IDs of the NAS servers on the system.
-pool	Type the name of the storage pool that the file system will use. **Note** Value is case-insensitive. View storage pools on page 194 explains how to view the names of the storage pools on the system.
-size	Type the quantity of storage to reserve for the file system. Storage resource size limitations on page 368 explains the limitations on storage size.
-thin	Enable thin provisioning on the file system. Value is yes or no. Default is no.
-type	Specify the type of network shares to export from the file system. Value is one of the following: • nfs — Network shares for Linux/UNIX hosts. • cifs — Network shares for Windows hosts. • multiprotocol — Network shares for multiprotocol sharing. **Note** Values are case-insensitive.
-cifsSyncWrites	Enable synchronous write operations for CIFS network shares. Value is yes or no. Default is no.
-cifsOpLocks	Enable opportunistic file locks (oplocks) for CIFS network shares. Value is yes or no. Default is yes.

Qualifier	Description
`-cifsNotifyOnWrite`	Enable to receive notifications when users write to a CIFS share. Value is yes or no. Default is no.
`-cifsNotifyOnAccess`	Enable to receive notifications when users access a CIFS share. Value is yes or no. Default is no.
`-cifsNotifyDirDepth`	If the value for `-cifsNotifyOnWrite` or `-cifsNotifyOnAccess` is yes (enabled), specify the subdirectory depth to which the notifications will apply. Value range is within range 1–512. Default is 512.
`-accessPolicy`	Access policy type for this file system. Valid values (case insensitive): • `native` (default) • `Unix` • `Windows`
`-fileLevelRet`	Enable file-level retention on the file system. Values is yes or no. Default is no.
`-sched`	Type the ID of a protection schedule to apply to the storage resource. View protection schedules on page 55 explains how to view the IDs of the schedules on the system.
`-schedPaused`	Specify whether to pause the protection schedule specified for -sched. Value is yes or no.

Example

The following command creates a file system with these settings:

- Name is FileSystem01.
- Description is "NFS shares."
- Uses the capacity storage pool.
- Uses NAS server NAS_1 as the primary NAS server.
- Primary storage size is 100 MB.
- Supports NFS network shares.

The file system receives the ID FS_1:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs create -name FileSystem01 -descr "NFS shares" -pool capacity -server nas_1 - size 100M -type nfs`

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = FS_1
Operation completed successfully.
```

View file systems

View details about a file system. You can filter on the file system ID.

Format
```
/stor/prov/fs [-id <value>] show
```

Object qualifier

Qualifier	Description
-id	Type the ID of a file system.

Example
The following command lists details about all file ssytems on the system:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID                    = fs1
        Name                  = MyFS
        Description           = my file system
        Health state          = OK (5)
        File system           = FS_1
        Server                = nas_1
        Storage pool          = Performance
        Protocol              = nfs
        Size                  = 1099511627776 (1T)
        Size used             = 128849018880 (120G)
        Protection size used  = 1099511627776 (1T)
        Deduplication enabled = no
```

Change file system settings

Change the settings for a file system.

Format
```
/stor/prov/fs -id <value> set [-async] [-descr <value>] [-size
<value>] [-thin {yes | no}] [-cifsSyncWrites {yes | no}] [-
fastvpPolicy { startHighThenAuto | auto | highest | lowest |
none}] [-cifsOpLocks {yes | no}] [-cifsNotifyOnWrite {yes |
no}] [-cifsNotifyOnAccess {yes | no}] [-cifsNotifyDirDepth
<value>] [{-sched <value> | -noSched}] [-schedPaused {yes |
no}]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the file system to change.

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.
-descr	Type a brief description of the file system.
-size	Type the amount of storage in the pool to reserve for the file system. Storage resource size limitations on page 368 explains the limitations on storage size.
-thin	Enable thin provisioning on the file system. Value is yes or no. Default is no.
-cifsSyncWrites	Enable synchronous write operations for CIFS network shares. Value is yes or no. Default is no.
-cifsOpLocks	Enable opportunistic file locks (oplocks) for CIFS network shares. Value is yes or no. Default is yes.
-cifsNotifyOnWrite	Enable to receive notifications when users write to a CIFS share. Value is yes or no. Default is no.
-cifsNotifyOnAccess	Enable to receive notifications when users access a CIFS share. Value is yes or no. Default is no.
-cifsNotifyDirDepth	If the value for -cifsNotifyOnWrite or -cifsNotifyOnAccess is yes (enabled), specify the subdirectory depth to which the notifications will apply. Value range is 1–512. Default is 512.
-sched	Type the ID of the schedule to apply to the file system. View protection schedules on page 55 explains how to view the IDs of the schedules on the system.
-schedPaused	Pause the schedule specified for the -sched qualifier. Value is yes or no (default).
-noSched	Unassigns the protection schedule.
-fastvpPolicy	Specify the FAST VP policy of the file system. Value is one of the following: • startHighThenAuto • auto • highest • lowest

Example
The following command enables thin provisioning on file system FS_1:

**uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs –id
FS_1 set -thin yes**

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = FS_1
Operation completed successfully.
```

Delete file systems

Delete a file system.

Note

Deleting a file system removes all network shares, and optionally snapshots associated with the file system from the system. After the file system is deleted, the files and folders inside it cannot be restored from snapshots. Back up the data from a file system before deleting it from the system.

Format
```
/stor/prov/fs -id <value> delete [-deleteSnapshots {yes | no}]
[-async]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the file system to delete.

Action qualifier

Qualifier	Description
-deleteSnapshots	Specifies that snapshots of the file system can be deleted along with the file system itself. Value is one of the following: • Yes • No Default value is no.
-async	Run the operation in asynchronous mode.

Example
The following command deletes file system FS_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs -id FS_1 delete

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage NFS network shares

Network file system (NFS) network shares use the NFS protocol to provide an access point for configured Linux/UNIX hosts, or IP subnets, to access file system storage. NFS network shares are associated with an NFS file system.

Each NFS share is identified by an ID.

The following table lists the attributes for NFS network shares:

Table 75 NFS network share attributes

Attribute	Description
ID	ID of the share.
Name	Name of the share.
Description	Brief description of the share.
Local path	Name of the directory on the system where the share resides.
Export path	Export path, used by hosts to connect to the share. **Note** The export path is a combination of the name of the associated NAS server and the name of the share.
File system	ID of the parent file system associated with the NFS share.
Default access	Default share access settings for host configurations and for unconfigured hosts that can reach the share. Value is one of the following: • `ro` - Read-only access to primary storage and snapshots associated with the share. • `rw` - Read/write access to primary storage and snapshots associated with the share. • `root` - Read/write root access to primary storage and snapshots associated with the share. This includes the ability to set access controls that restrict the permissions for other login accounts. • `na` - No access to the share or its snapshots.
Read-only hosts	ID of each host that has read-only permission to the share and its snapshots.
Read/write hosts	ID of each host that has read/write permissions to the share and its snapshots.
Root hosts	ID of each host that has root permission to the share and its snapshots.
No access hosts	ID of host that has no access to the share or its snapshots.
Creation time	Creation time of the share.
Last modified time	Last modified time of the share.

Create NFS network shares

Create an NFS share to export a file system through the NFS protocol.

Note

Share access permissions set for specific hosts take effect only if the host-specific setting is less restrictive than the default access setting for the share. Additionally, setting access for a specific host to "No Access" always takes effect over the default access setting.

- Example 1: If the default access setting for a share is Read-Only, setting the access for a specific host configuration to Read/Write will result in an effective host access of Read/Write.

- Example 2: If the default access setting for the share is Read-Only, setting the access permission for a particular host configuration to No Access will take effect and prevent that host from accessing to the share.

- Example 3: If the default access setting for a share is Read-Write, setting the access permission for a particular host configuration to Read-Only will result in an effective host access of Read/Write.

Prerequisite

Configure a file system to which to associate the NFS network shares. explains how to create file systems on the system.

Format

```
/stor/prov/fs/nfs create [-async] –name <value> [-descr
<value>] –fs <value> -path <value> [-defAccess {ro|rw|root|na}]
[-roHosts <value>] [-rwHosts <value>] [-rootHosts <value>] [-
naHosts <value>]
```

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.
-name	Type a name for the share. **Note** This value, along with the name of the NAS server, constitutes the export path by which hosts access the share.
-descr	Type a brief description of the share.
-fs	Type the ID of the parent file system associated with the NFS share.
-path	Type a name for the directory on the system where the share will reside. This path must correspond to an existing directory/folder name within the share that was created from the host-side. • Each share must have a unique local path. The system automatically creates this path for the initial share created when you create the file system. • Before you can create additional network shares within an NFS file system, you must create network shares within it from a Windows host that is connected to the file system. After a share has been created from a mounted host, you can create a corresponding share on the system and set access permissions accordingly.

Qualifier	Description
-defAccess	Specify the default share access settings for host configurations and for unconfigured hosts that can reach the share. Value is one of the following: • `ro` — Read-only access to primary storage and snapshots associated with the share. • `rw` — Read/write access to primary storage and snapshots associated with the share. • `root` — Read/write root access to primary storage and snapshots associated with the share. This includes the ability to set access controls that restrict the permissions for other login accounts. • `na` — No access to the share or its snapshots.
-roHosts	Type the ID of each host configuration you want to grant read-only permission to the share and its snapshots. Separate each ID with a comma. • For host configurations of type 'host,' by default, all of the host's IP addresses can access the share and its snapshots. To allow access to only specific IPs, type those specific IPs in square brackets after the host ID. For example: ID[IP,IP], where 'ID' is a host configuration ID and 'IP' is an IP address. • View host configurations on page 144 explains how to view the ID of each host configuration.
-rwHosts	Type the ID of each host configuration you want to grant read-write permission to the share and its snapshots. Separate each ID with a comma. • For host configurations of type 'host,' by default, all of the host's IP addresses can access the share and its snapshots. To allow access to only specific IPs, type those specific IPs in square brackets after the host ID. For example: ID[IP,IP], where 'ID' is a host configuration ID and 'IP' is an IP address. • View host configurations on page 144 explains how to view the ID of each host configuration.
-rootHosts	Type the ID of each host configuration you want to grant root permission to the share and its snapshots. Separate each ID with a comma. • For host configurations of type 'host,' by default, all of the host's IP addresses can access the share and its snapshots. To allow access to only specific IPs, type those specific IPs in square brackets after the host ID. For example: ID[IP,IP], where 'ID' is a host configuration ID and 'IP' is an IP address. • View host configurations on page 144 explains how to view the ID of each host configuration.
-naHosts	Type the ID of each host configuration you want to block access to the share and its snapshots. Separate each ID with a comma. • For host configurations of type 'host,' by default, all of the host's IP addresses cannot access the share and its snapshots. To limit access for specific IPs, type the IPs in square brackets after the host

Qualifier	Description
	ID. For example: ID[IP,IP], where 'ID' is a host configuration ID and 'IP' is an IP address.
	• View host configurations on page 144 explains how to view the ID of each host configuration.

Example

The following command creates an NFS share with these settings:

- Name is NFSshare.

- Description is "My share."

- Associated to file system fs1.

- Local path on the system is directory nfsshare.

- Host HOST_1 has read-only permissions to the share and its snapshots.

- Hosts HOST_2 and HOST_3 have read and write access to the share and its snapshots.

The share receives ID NFS_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs/nfs
create –name NFSshare -descr "My share" –res fs1 -path "nfsshare"
HOST_1 -rwHosts "HOST_2,HOST_3"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = NFS_1
Operation completed successfully.
```

View NFS share settings

View details of an NFS share. You can filter on the NFS share ID or view the NFS network shares associated with a file system ID.

Note

The show action command on page 17 explains how to change the output format.

Format
```
/stor/prov/fs/nfs [{-id <value>|-fs <value>}] show
```

Object qualifier

Qualifier	Description
-id	Type the ID of an NFS share.
-fs	Type the ID of an NFS file system to view the associated NFS network shares.

Example

The following command lists details for all NFS network shares on the system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs/nfs
show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID              = NFS_1
        Name            = MyNFSshare1
        Description     = My nfs share
        Resource        = fs1
        Local path      = nfsshare1
        Export path     = 10.64.75.10/MyNFSshare1
        Default access  = na
        Read-only hosts = 1014, 1015
        Read/write hosts = 1016
        Root hosts      =
        No access hosts =


2:      ID              = NFS_2
        Name            = MyNFSshare2
        Description     = This is my second share
        Resource        = fs1
        Local path      = nfsshare2
        Export path     = 10.64.75.10/MyNFSshare2
        Default access  = na
        Read-only hosts = 1014, 1015
        Read/write hosts = 1016
        Root hosts      =
        No access hosts =
```

Change NFS share settings

Change the settings of an NFS share.

Format

```
/stor/prov/fs/nfs -id <value> set [-async][-descr <value>] [-
defAccess {ro|rw|root|na}] [-roHosts <value>] [-rwHosts
<value>] [-rootHosts <value>] [-naHosts <value>]
```

Object qualifier

Qualifier	Description
-id	Type the ID of an NFS share to change. View NFS share settings on page 230 explains how to view the IDs of the NFS network shares on the system.

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.
-descr	Type a brief description of the share.
-defAccess	Specify the default share access settings for host configurations and for unconfigured hosts who can reach the share. Value is one of the following: • `ro` – Read-only access to primary storage and snapshots associated with the share.

Qualifier	Description
	• `rw` – Read/write access to primary storage and snapshots associated with the share.
	• `root` – Read/write root access to primary storage and snapshots associated with the share. This includes the ability to set access controls that restrict the permissions for other login accounts.
	• `na` – No access to the share or its snapshots.
`-roHosts`	Type the ID of each host configuration you want to grant read-only permission to the share and its snapshots. Separate each ID with a comma. • For host configurations of type 'host,' by default, all of the host's IP addresses can access the share and its snapshots. To allow access to only specific IPs, type those specific IPs in square brackets after the host ID. For example: ID[IP,IP], where 'ID' is a host configuration ID and 'IP' is an IP address. • View host configurations on page 144 explains how to view the ID of each host configuration.
`-rwHosts`	Type the ID of each host configuration you want to grant read-write permission to the share and its snapshots. Separate each ID with a comma. • For host configurations of type 'host,' by default, all of the host's IP addresses can access the share and its snapshots. To allow access to only specific IPs, type those specific IPs in square brackets after the host ID. For example: ID[IP,IP], where 'ID' is a host configuration ID and 'IP' is an IP address. • View host configurations on page 144 explains how to view the ID of each host configuration.
`-rootHosts`	Type the ID of each host configuration you want to grant root permission to the share and its snapshots. Separate each ID with a comma. • For host configurations of type 'host,' by default, all of the host's IP addresses can access the share and its snapshots. To allow access to only specific IPs, type those specific IPs in square brackets after the host ID. For example: ID[IP,IP], where 'ID' is a host configuration ID and 'IP' is an IP address. • View host configurations on page 144 explains how to view the ID of each host configuration.
`-naHosts`	Type the ID of each host configuration you want to block access to the share and its snapshots. Separate each ID with a comma. • For host configurations of type 'host,' by default, all of the host's IP addresses cannot access the share and its snapshots. To limit access for specific IPs, type the IPs in square brackets after the host ID. For example: ID[IP,IP], where 'ID' is a host configuration ID and 'IP' is an IP address. • View host configurations on page 144 explains how to view the ID of each host configuration.

Example

The following command changes NFS share NFS_1 to block access to the share and its snapshots for host HOST_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs/nfs –id NFS_1 set -descr "My share" -naHosts "HOST_1"

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = NFS_1
Operation completed successfully.
```

Delete NFS network shares

Delete an NFS share.

Note

Deleting a share removes any files and folders associated with the share from the system. You cannot use snapshots to restore the contents of a share. Back up the data from a share before deleting it from the system.

Format
`/stor/prov/fs/nfs –id <value> delete [-async]`

Object qualifier

Qualifier	Description
–id	Type the ID of an NFS share to change. View NFS share settings on page 230 explains how to view the IDs of the NFS network shares on the system.

Action qualifier

Qualifier	Description
–async	Run the operation in asynchronous mode.

Example

The following command deletes NFS share NFS_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs/nfs –id NFS_1 delete

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage CIFS network shares

Common internet file system (CIFS) network shares use the CIFS protocol to provide an access point for configured Windows hosts, or IP subnets, to access file system storage. CIFS network shares are associated with a CIFS file system.

Each CIFS share is identified by an ID.

The following table lists the attributes for CIFS network shares:

Table 76 CIFS network share attributes

Attribute	Description
ID	ID of the share.
Name	Name of the share.
Description	Brief description of the share.
Local path	Name of the directory on the system where the share resides.
Export path	Export path, used by hosts to connect to the share. **Note** The export path is a combination of the name of the associated NAS server and the name of the share.
File system	ID of the parent file system associated with the CIFS share.
Creation time	Creation time of the share.
Last modified time	Last modified time of the share.
Availability enabled	Continuous availability state.
Encryption enabled	CIFS encryption state.
Umask	Indicates the default Unix umask for new files created on the share. If not specified, the umask defaults to 022.
ABE enabled	Indicates whether an Access-Based Enumeration (ABE) filter is enabled. Valid values include: • yes — Filters the list of available files and folders on a share to include only those that the requesting user has access to. • no (default)
DFS enabled	Indicates whether Distributed File System (DFS) is enabled. Valid values include: • yes — Allows administrators to group shared folders located on different shares by transparently connecting them to one or more DFS namespaces. • no (default)
BranchCache enabled	Indicates whether BranchCache is enabled. Valid values include: • yes — Copies content from the main office or hosted cloud content servers and caches the content at branch office locations. This allows client computers at branch offices to access content locally rather than over the WAN. • no (default)

Table 76 CIFS network share attributes (continued)

Attribute	Description
Offline availability	Indicates whether Offline availability is enabled. When enabled, users can use this feature on their computers to work with shared folders stored on a server, even when they are not connected to the network. Valid values include: • none — Prevents clients from storing documents and programs in offline cache. (default) • documents — All files that clients open from the share will be available offline. • programs — All programs and files that clients open from the share will be available offline. Programs and files will preferably open from offline cache, even when connected to the network. • manual — Only specified files will be available offline.

Create CIFS network shares

Create a CIFS share to export a file system through the CIFS protocol.

Prerequisite

Configure a file system to which to associate the CIFS network shares. Create file systems on page 221 explains how to create file systems on the system.

Format

```
/stor/prov/fs/cifs create [-async] –name <value> [-descr
<value>] –fs <value> -path <value> [-
enableContinuousAvailability {yes|no}] [-enableCIFSEncryption
{yes|no}] [-umask <value> ] [-enableABE {yes | no} ] [-
enableBranchCache {yes | no}] [-offlineAvailability {none |
documents | programs | manual} ]
```

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.
-name	Type a name for the share. **Note** This value, along with the name of the NAS server, constitutes the export path by which hosts access the share.
-descr	Type a brief description of the share.
-fs	Type the ID of the parent file system associated with the CIFS share.
-path	Type a name for the directory on the system where the share will reside. This path must correspond to an existing directory/folder

Qualifier	Description
	name within the share that was created from the host-side.
	• Each share must have a unique local path. The system automatically creates this path for the initial share created when you create the file system.
	• Before you can create additional network shares within an NFS file system, you must create network shares within it from a Windows host that is connected to the file system. After a share has been created from a mounted host, you can create a corresponding share on the system and set access permissions accordingly.
`-enableContinuousAvailability`	Specify whether continuous availability is enabled.
`-enableCIFSEncryption`	Specify whether CIFS encryption is enabled.
`-umask`	Type the default Unix umask for new files created on the share.
`-enableABE`	Specify if Access-based Enumeration (ABE) is enabled. Valid values include: • `yes` • `no`
`-enableBranchCache`	Specify if BranchCache is enabled. Valid values include: • `yes` • `no`
`-offlineAvailability`	Specify the type of offline availability. Valid values include: • `none` (default) — Prevents clients from storing documents and programs in offline cache. • `documents` — Allows all files that clients open to be available offline. • `programs` — Allows all programs and files that clients open to be available offline. Programs and files will open from offline cache, even when connected to the network. • `manual` — Allows only specified files to be available offline.

Example
The following command creates a CIFS share with these settings:

- Name is CIFSshare.
- Description is **"My share."**
- Associated to file system fs1.
- Local path on the system is directory cifsshare.
- Continuous availability is enabled.
- CIFS encryption is enabled.

The share receives ID CIFS_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs/cifs create –name CIFSshare -descr "My share" –fs fs1 -path "cifsshare" - enableContinuousAvailability yes -enableCIFSEncryption yes

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = CIFS_1
Operation completed successfully.
```

View CIFS share settings

View details of a CIFS share. You can filter on the CIFS share ID or view the CIFS network shares associated with a file system ID.

Note

The show action command on page 17 explains how to change the output format.

Format
/stor/prov/fs/cifs [{-id *<value>*|-fs *<value>*}] show

Object qualifier

Qualifier	Description
-id	Type the ID of a CIFS share.
-fs	Type the ID of an CIFS file system to view the associated CIFS network shares.

Example
The following command lists details for all NFS network shares on the system:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs/cifs show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID          = CIFS_1
        Name        = MyCIFSshare1
        Description = This is my CIFS share
        File system = fs1
        Local path  = cifsshare1
        Export path = 10.64.75.10/MyCIFSshare1

2:      ID          = CIFS_2
        Name        = MyCIFSshare2
        Description = This is my second share
```

```
         File system  = fs1
         Local path   = cifsshare2
         Export path  = 10.64.75.10/MyCIFSshare2
```

Change CIFS share settings

Change the settings of an CIFS share.

Format

/stor/prov/fs/cifs –id *<value>* set [-async] –name *<value>* [-
descr *<value>*] [-enableContinuousAvailability {yes|no}] [-
enableCIFSEncryption {yes|no}] [-umask *<value>*] [-enableABE
{yes | no}] [-enableBranchCache {yes | no}] [-
offlineAvailability {none | documents | programs | manual}]

Object qualifier

Qualifier	Description
–id	Type the ID of a CIFS share to change.

Action qualifier

Qualifier	Description
–async	Run the operation in asynchronous mode.
–descr	Specifies the description for the CIFS share.
–enableContinuousAvailability	Specifies whether continuous availability is enabled.
–enableCIFSEncryption	Specifies whether CIFS encryption is enabled.
–umask	Type the default Unix umask for new files created on the share.
–enableABE	Specify if Access-Based Enumeration (ABE) is enabled. Valid values include: • yes • no
–enableBranchCache	Specify if BranchCache is enabled. Valid values include: • yes • no
–offlineAvailability	Specify the type of offline availability. Valid values include: • none (default) — Prevents clients from storing documents and programs in offline cache. • documents — Allows all files that users open to be available offline.

Qualifier	Description
	• `programs` — Allows all programs and files that users open to be available offline. Programs and files will open from offline cache, even when connected to the network. • `manual` — Allows only specified files to be available offline.

Example

The following command sets the description of CIFS share CIFS_1 to `My share`.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs/cifs –id CIFS_1 set -descr "My share"

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = CIFS_1
Operation completed successfully.
```

Delete CIFS network shares

Delete a CIFS share.

Note

Deleting a share removes any files and folders associated with the share from the system. You cannot use snapshots to restore the contents of a share. Back up the data from a share before deleting it from the system.

Format
`/stor/prov/fs/cifs –id <value> delete [-async]`

Object qualifier

Qualifier	Description
`–id`	Type the ID of a CIFS share to change.

Action qualifier

Qualifier	Description
`–async`	Run the operation in asynchronous mode.

Example

The following command deletes CIFS share CIFS_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/sf/cifs –id CIFS_1 delete

```
Storage system address: 10.0.0.1
Storage system port: 443
```

```
HTTPS connection

Operation completed successfully.
```

Manage LUNs

A LUN is a single unit of storage that represents a specific storage pool and quantity of Fibre Channel (FC) or iSCSI storage. Each LUN is associated with a name and logical unit number (LUN) identifier.

Each LUN is identified by an ID.

The following table lists the attributes for LUNs:

Table 77 LUN attributes

Attribute	Description
ID	ID of the LUN.
Name	Name of the LUN.
Description	Brief description of the LUN.
Storage pool ID	ID of the storage pool the LUN is using.
Storage pool	Name of the storage pool the LUN is using.
Health state	Health state of the LUN storage. The health state code appears in parentheses. Value is one of the following: • `OK (5)` — The LUN storage is operating normally. • `Degraded/Warning (10)` — Working, but one or more of the following may have occurred: ▪ One or more of its storage pools are degraded. ▪ Resource is degraded. ▪ Resource is running out of space and needs to be increased. • `Minor failure (15)` — One or both of the following may have occurred: ▪ One or more of its storage pools have failed. ▪ Resource is unavailable. • `Major failure (20)` — One or both of the following may have occurred: ▪ One or more of its storage pools have failed. ▪ Resource is unavailable. • `Critical failure (25)` — One or more of the following may have occurred: ▪ One or more of its storage pools are unavailable. ▪ Resource is unavailable. ▪ Resource has run out of space and needs to be increased. • `Non-recoverable error (30)` — One or both of the following may have occurred:

Table 77 LUN attributes (continued)

Attribute	Description
	▪ One or more of its storage pools are unavailable. ▪ Resource is unavailable.
Health details	Additional health information.
Size	Current size of the LUN.
Maximum size	Maximum size of the LUN.
Thin provisioning enabled	Indication of whether thin provisioning is enabled. Value is yes or no. Default is no. All storage pools support both standard and thin provisioned storage resources. For standard storage resources, the entire requested size is allocated from the pool when the resource is created, for thin provisioned storage resources only incremental portions of the size are allocated based on usage. Because thin provisioned storage resources can subscribe to more storage than is actually allocated to them, storage pools can be over provisioned to support more storage capacity than they actually possess. **Note** The Unisphere online help provides more details on thin provisioning.
Current allocation	If thin provisioning is enabled, the quantity of primary storage currently allocated through thin provisioning.
Protection size used	Quantity of storage currently used for protection data.
Snapshot count	Number of snapshots created on the LUN.
Protection schedule	ID of a protection schedule applied to the VMFS datastore . View protection schedules on page 55 explains how to view the IDs of the schedules on the system.
Protection schedule paused	Indication of whether an applied protection schedule is currently paused.
WWN	World Wide Name of the LUN.
Creation time	The time the resource was created.
Last modified time	The time resource was last modified.
SP owner	Indicates the default owner of the LUN. Value is one of the following: ● SP A ● SP B
Trespassed	Indicates whether the LUN is trespassed to the peer SP. Value is one of the following: ● Yes ● No
FAST VP policy	FAST VP policy of the LUN storage. Value is one of the following:

Table 77 LUN attributes (continued)

Attribute	Description
	• `Start high then auto-tier` • `Auto-tier` • `Highest available tier` • `Lowest available tier`
`FAST VP distribution`	Percentage of the LUN storage assigned to each tier. The format is: `<tier_name>:<value>%` where, *‹tier_name›* is the name of the storage tier and *‹value›* is the percentage of storage in that tier.
`LUN access hosts`	List of hosts with access permissions to the LUN.
`Snapshots access hosts`	List of hosts with access to snapshots of the LUN.

Create LUNs

Create a LUN to which host initiators connect to access storage.

Prerequisites

Configure at least one storage pool for the LUN to use and allocate at least one storage disk to the pool. Configure storage pools automatically (physical deployments only) on page 186 explains how to create storage pools automatically on the system and Configure custom storage pools on page 188 explains how to create a custom storage pool on the system.

Format

```
/stor/prov/luns/lun create [-async] -name <value> [-descr
<value>] [-group <value>] -pool <value> -size <value> -thin
{yes | no} [-sched <value> [-schedPaused {yes | no}]] [-
fastvpPolicy { startHighThenAuto | auto | highest | lowest }]
[ -lunHosts <value>] [ -snapHosts <value>]
```

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-name`	Type the name of the LUN.
`-descr`	Type a brief description of the LUN.
`-group`	Type the ID of a LUN group to associate the new LUN with. View LUN groups on page 250 explains how to view information on LUN groups. **Note** If no LUN group is specified, the LUN will not be assigned to a LUN group.

Qualifier	Description
-pool	Type the name of the storage pool that the LUN will use. **Note** Value is case-insensitive. View storage pools on page 194 explains how to view the names of the storage pools on the system.
-size	Type the quantity of storage to allocate for the LUN. Storage resource size limitations on page 368 explains the limitations on storage size.
-thin	Enable thin provisioning on the LUN. Value is yes or no. Default is no.
-sched	Type the ID of a protection schedule to apply to the storage resource. View protection schedules on page 55 explains how to view the IDs of the schedules on the system.
-schedPaused	Pause the schedule specified for the -sched qualifier. Value is yes or no. Default is no.
-fastvpPolicy	Specify the FAST VP policy of the LUN. Value is one of the following: • startHighThenAuto • auto • highest • lowest
-lunHosts	Specifies a comma-separated list of hosts with access to the LUN.
-snapHosts	Specifies a comma-separated list of hosts with access to snapshots of the LUN.

Example

The following command creates a LUN with these settings:

- Name is MyLUN.
- Description is "My LUN."
- Associated with LUN group group_1.
- Uses the pool_1 storage pool.
- Primary storage size is 100 MB.

The LUN receives the ID lun_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/lun create -name "MyLUN" -descr "My LUN" -group group_1 -pool pool_1 -size 100M

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = lun_1
Operation completed successfully.
```

View LUNs

Display the list of existing LUNs.

Note

The show action command on page 17 explains how to change the output format.

Format

```
/stor/prov/luns/lun [{-id <value> | -group <value> | -
standalone}] show
```

Object qualifier

Qualifier	Description
-id	Type the ID of a LUN.
-group	Type the name of a LUN group. The list of LUNs in the specified LUN group are displayed.
-standalone	Displays only LUNs that are not part of a LUN group.

Example

The following command displays details about all LUNs on the system:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/lun
show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID                   = lun_1
        Name                 = MyLUN
        Description          = My LUN
        Group                = group_1
        Storage pool ID      = pool_1
        Storage pool         = Capacity
        Health state         = OK (5)
        Size                 = 2199023255552 (2T)
        Protection size used = 0
        SP owner             = SPA
        Trespassed           = no

2:      ID                   = lun_2
        Name                 = MyLUN2
        Description          = My second LUN
        Group                = group_1
        Storage pool ID      = pool_2
        Storage pool         = Performance
        Health state         = OK (5)
        Size                 = 104857600 (100M)
        Protection size used = 0
        SP owner             = SPB
        Trespassed           = no
```

Change LUNs

Change the settings for a LUN.

Format

```
/stor/prov/luns/lun -id <value> set [-async] [-name <value>] [-
descr <value>] [-size <value>] [{-group <value> | -standalone}]
```

```
[{-sched <value> | -noSched}] [-schedPaused {yes | no}] [-
spOwner {spa | spb}] [-fastvpPolicy { startHighThenAuto | auto
| highest | lowest | none}] [ -lunHosts <value>] [ -snapHosts
<value>]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the LUN to change.

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.
-name	Type the name of the LUN.
-descr	Type a brief description of the LUN.
-group	Type the ID of a LUN group to associate the new LUN with. View LUN groups on page 250 explains how to view information on LUN groups. **Note** If no LUN group is specified, the LUN will not be assigned to a LUN group.
-size	Type the quantity of storage to allocate for the LUN. Storage resource size limitations on page 368 explains the limitations on storage size.
-standalone	Removes the LUN from the LUN group.
-sched	Type the ID of the schedule to apply to the NFS datastore. View protection schedules on page 55 explains how to view the IDs of the schedules on the system.
-schedPaused	Pause the schedule specified for the -sched qualifier. Value is yes or no. Default is no.
-noSched	Unassigns the protection schedule.
-spOwner	Specifies the default owner of the LUN. Value is one of the following: • SP A • SP B
-fastvpPolicy	Specify the FAST VP policy of the LUN storage. Value is one of the following: • startHighThenAuto • auto • highest • lowest

Qualifier	Description
-lunHosts	Specifies a comma-separated list of hosts with access to the LUN.
-snapHosts	Specifies a comma-separated list of hosts with access to snapshots of the LUN.

Example

The following command updates LUN lun_1with these settings:

- Name is NewName.
- Description is "My new description."
- Primary storage size is 150 MB.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/lun -id lun_1 set -name NewName -descr "My new description" -size 150M

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = lun_1
Operation completed successfully.
```

Delete LUNs

Delete a LUN.

Note

Deleting a LUN removes all associated data from the system. After a LUN is deleted, you cannot restore the data inside it from snapshots. Back up the data from a LUN to another host before deleting it from the system.

Format

/stor/prov/luns/lun -id <value> delete [-deleteSnapshots {yes | no}] [-async]

Object qualifier

Qualifier	Description
-id	Type the ID of the LUN to delete.

Action qualifier

Qualifier	Description
-deleteSnapshots	Specifies that snapshots of the LUN can be deleted along with the LUN itself. Value is one of the following: - Yes - No (default)
-async	Run the operation in asynchronous mode.

Example

The following command deletes LUN lun_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/lun
-id lun_1 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage LUN groups

LUN groups provide a way to organize and group LUNs together to simplify storage tiering and snapshots when an application spans multiple LUNs.

The following table lists the attributes for LUN groups:

Table 78 LUN group attributes

Attribute	Description
ID	ID of the LUN.
Name	Name of the LUN.
Description	Brief description of the LUN.

Health state	Health state of the LUN storage. The health state code appears in parentheses. Value is one of the following:
	
	• OK (5) — The LUN storage is operating normally.
	
	• Degraded/Warning (10) - Working, but one or more of the following may have occurred:
	  ▪ One or more of its storage pools are degraded.
	  ▪ Resource is degraded.
	  ▪ Resource is running out of space and needs to be increased.
	
	• Minor failure (15) — One or both of the following may have occurred:
	  ▪ One or more of its storage pools have failed.
	  ▪ Resource is unavailable.
	
	• Major failure (20) — One or both of the following may have occurred:
	  ▪ One or more of its storage pools have failed.
	  ▪ Resource is unavailable.
	
	• Critical failure (25) — One or more of the following may have occurred:
	  ▪ One or more of its storage pools are unavailable.
	  ▪ Resource is unavailable.
	  ▪ Resource has run out of space and needs to be increased.
	
	• Non-recoverable error (30) — One or both of the following may have occurred:
	  ▪ One or more of its storage pools are unavailable.

Table 78 LUN group attributes (continued)

Attribute	Description
	■ Resource is unavailable.
Health details	Additional health information. See Appendix A, Reference, for health information details.
Total capacity	Total capacity of all associated LUNs.
Total current allocation	Total current allocation of all associated LUNs.
Thin provisioning enabled	Indication of whether thin provisioning is enabled. Value is yes or no. Default is no. All storage pools support both standard and thin provisioned storage resources. For standard storage resources, the entire requested size is allocated from the pool when the resource is created, for thin provisioned storage resources only incremental portions of the size are allocated based on usage. Because thin provisioned storage resources can subscribe to more storage than is actually allocated to them, storage pools can be over provisioned to support more storage capacity than they actually possess. **Note** The Unisphere online help provides more details on thin provisioning.
Total protection size used	Total quantity of storage used for protection data.
Snapshot count	Number of snapshots created on the LUN.
Protection schedule	ID of a protection schedule applied to the VMFS datastore . View protection schedules on page 55 explains how to view the IDs of the schedules on the system.
Protection schedule paused	Indication of whether an applied protection schedule is currently paused.
LUN access hosts	List of hosts with access permissions to the associated LUNs. **Note** Hosts that have access to the snapshots of some, but not all of the associated LUNs are marked as Mixed.
Snapshots access hosts	List of hosts with access to snapshots of the associated LUNs. **Note** Hosts that have access to the snapshots of some, but not all of the associated LUNs are marked as **Mixed**.
Replication destination	Indication of whether the LUN group is a destination for a replication session (local or remote). Value is yes or no. Manage replication sessions on page 304 explains how to configure replication sessions on the system.
Creation time	The time the resource was created.

Table 78 LUN group attributes (continued)

Attribute	Description
Last modified time	The time resource was last modified.
FAST VP policy	FAST VP policy of the LUN storage. Value is one of the following: • `Start high then auto-tier` • `Auto-tier` • `Highest available tier` • `Lowest available tier`
FAST VP distribution	Percentage of the LUN storage assigned to each tier. The format is: `<tier_name>:<value>%` where, *tier_name* is the name of the storage tier and *value* is the percentage of storage in that tier.

Create a LUN group

Create a LUN group.

Format

```
/stor/prov/luns/group create [-async] -name <value> [-descr
<value>] [-sched <value> [-schedPaused {yes | no}]] [-replDest
{yes | no}]
```

Action qualifier

Qualifier	Description
-async	Run the operation is asynchronous mode.
-name	Type a name for the storage resource. **Note** Use a name that reflects the type and version of the application that will use it, which can facilitate how the storage resource is managed and monitored through Unisphere.
-descr	Type a brief description of the storage resource.
-sched	Type the ID of a protection schedule to apply to the storage resource. View protection schedules on page 55 explains how to view the IDs of the schedules on the system.
-schedPaused	Specify whether to pause the protection schedule specified for -sched. Value is yes or no.
-replDest	Specifies whether the resource is a replication destination. Valid values are: • `Yes`

Qualifier	Description
	• `No` (default) **Note** Values are case insensitive.

Example

The following command creates a LUN group with these settings:

- Name is GenericStorage01.
- Description is "MyStorage."
- Uses protection schedule SCHD_1.

The storage resource receives the group_1:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/`
`group create -name GenericStorage01 -descr "MyStorage" -sched SCHD_1`

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = group_1
Operation completed successfully.
```

View LUN groups

Display the list of existing LUN groups.

Note

explains how to change the output format.

Format
`/stor/prov/luns/group -id <value> show`

Object qualifier

Qualifier	Description
`-id`	Type the ID of a LUN group.

Example

The following command displays details about the LUN group on the system:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/`
`group show -detail`

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:     ID                     = group_1
       Name                   = MyLUNGroup
       Description            = My LUN group
       Health state          = OK (5)
       Health details        = "The component is operating
```

```
normally.  No action is required."
        Total capacity            = 107374182400 (100G)
        Thin provisioning enabled  = no
        Total current allocation   = 107374182400 (100G)
        Total protection size used = 0
        Snapshot count             = 0
        Total current allocation   = 10737418240 (10G)
        Protection schedule        = SCHD_1
        Protection schedule paused = no
        LUNs access hosts          = 1014, 1015
        Snapshots access hosts     = 1016(mixed)
        Creation time              = 2012-12-21 12:55:32
        Last modified time         = 2013-01-15 10:31:56
        FAST VP policy             = mixed
        FAST VP distribution       = Best Performance: 55%, High
Performance: 10%, High Capacity: 35%
```

Change LUN groups

Change the settings for a LUN group.

Format
```
/stor/prov/luns/group –id <value> set [-async] [-name <value>]
[-descr <value>] [{-sched <value> | -noSched}] [-schedPaused
{yes | no}] [-lunHosts <value>] [ -snapHosts <value>] [-
replDest {yes | no}] [-fastvpPolicy { startHighThenAuto | auto
| highest | lowest | none}]
```

Object qualifier

Qualifier	Description
–id	Type the ID of iSCSI storage resource to change.

Action qualifier

Qualifier	Description
–async	Run the operation in asynchronous mode.
–name	Type the name of the LUN.
–descr	Type a brief description of the LUN.
–sched	Type the ID of the schedule to apply to the LUN. View protection schedules on page 55 explains how to view the IDs of the schedules on the system.
–schedPaused	Pause the schedule specified for the –sched qualifier. Value is yes or no (default).
–noSched	Unassigns the protection schedule.
–lunHosts	Specifies a comma-separated list of hosts with access to the LUN.
–snapHosts	Specifies a comma-separated list of hosts with access to snapshots of the LUN.
–replDest	Specifies whether the resource is a replication destination. Valid values are: • Yes

Qualifier	Description
	• `No` (default)
	Note
	Values are case insensitive.
`-fastvpPolicy`	Specify the FAST VP policy of the LUN storage. Value is one of the following:
	• `startHighThenAuto`
	• `auto`
	• `highest`
	• `lowest`

Example

The following command updates the LUN group group_1 with these settings:

• Name is NewName.

• Description is "New description."

• Uses protection schedule SCHD_2.

• The selected schedule is currently paused.

• The FAST VP policy is start high then auto-tier.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/ group -id group_1 set -name NewName -descr "New description" -sched SCHD_2 -schedPaused yes -fastvpPolicy startHighThenAuto

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = group_1
Operation completed successfully.
```

Delete LUN groups

Delete a LUN group.

Note

Deleting a LUN group removes all LUNs and data associated with the LUN group from the system. After a LUN group is deleted, you cannot restore the data from snapshots. Back up the data from the LUN group before deleting it.

Format

```
/stor/prov/luns/group -id <value> delete -id <value> delete [-
async]
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the LUN to delete.

Action qualifier

Qualifier	Description
-deleteSnapshots	Specifies that snapshots of the LUN can be deleted along with the LUN itself. Value is one of the following: • Yes • No (default)
-async	Run the operation in asynchronous mode.

Example

The following command deletes LUN group storage resource group_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/ group -id group_1 delete

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage VMware NFS datastores

VMware NFS datastores provide file-based storage to VMware ESX Servers for hosting virtual machines (VM). You can provision and manage NFS datastores and view details about each NFS datastore on the system, such as their storage capacity and health.

Each NFS datastore is identified by an ID.

The following table lists the attributes for NFS datastores:

Table 79 NFS datastore attributes

Attribute	Description
ID	ID of the NFS datastore.
Name	Name of the NFS datastore.
Description	Description of the NFS datastore.

Health state	Health state of the NFS datastore. The health state code appears in parentheses. Value is one of the following:
	
	• OK (5) — NFS datastore is operating normally.
	
	• Degraded/Warning (10) — Working, but one or more of the following may have occurred:
	
	  ▪ One or more of its storage pools are degraded.
	
	  ▪ It has almost reached full capacity. Increase the primary storage size, or create additional NFS datastores to store your data, to avoid data loss. Change NFS datastore settings on page 260 explains how to change the primary storage size.
	
	• Minor failure (15) — One or both of the following may have occurred:

Table 79 NFS datastore attributes (continued)

Attribute	Description

	■ One or more of its storage pools have failed.
	
	    ■ The associated NAS server has failed.
	
	• `Major failure (20)` — One or both of the following may have occurred:
	
	    ■ One or more of its storage pools have failed.
	
	    ■ NFS datastore is unavailable.
	
	• `Critical failure (25)` — One or more of the following may have occurred:
	
	    ■ One or more of its storage pools are unavailable.
	
	    ■ NFS datastore is unavailable.
	
	    ■ NFS datastore has reached full capacity. Increase the primary storage size, or create additional NFS datastore to store your data, to avoid data loss. Change NFS datastore settings on page 260 explains how to change the primary storage size.
	
	• `Non-recoverable error (30)` — One or both of the following may have occurred:
	
	    ■ One or more of its storage pools are unavailable.
	
	    ■ NFS datastore is unavailable.

`Health details`	Additional health information. See Appendix A, Reference, for health information details.
`File system`	Identifier for the datastore. Output of some metrics commands display only the datastore ID. This will enable you to easily identify the datastore in the output.
`Server`	Name of the primary NAS server that the NFS datastore uses.
`Storage pool ID`	Identifier of the storage pool that the NFS datastore uses.
`Storage pool`	Name of the storage pool that the NFS datastore uses.
`Format`	Datastore format (applies to NFS datastores only). Valid values are: • `UFS32` - Indicates a 32-bit NFS datastore. • `UFS64` - Indicates a 64-bit NFS datastore.
`Size`	Quantity of storage reserved for primary data.
`Size used`	Quantity of storage currently used for primary data.
`Maximum size`	Maximum size to which you can increase the primary storage capacity.
`Thin provisioning enabled`	Indication of whether thin provisioning is enabled. Value is yes or no. Default is no. All storage pools support both standard and thin provisioned storage resources. For standard storage resources, the entire requested size is allocated from the pool when the resource is created, for thin provisioned storage resources only incremental portions of the size are allocated based on usage. Because thin provisioned storage resources can subscribe to more storage than is

Table 79 NFS datastore attributes (continued)

Attribute	Description
	actually allocated to them, storage pools can be over provisioned to support more storage capacity than they actually possess. **Note** The Unisphere online help provides more details on thin provisioning.
Current allocation	If enabled, the quantity of primary storage currently allocated through thin provisioning.
Protection size used	Quantity of storage currently used for protection data.
Snapshot count	Quantity of protection storage currently allocated through thin provisioning.
Protection schedule	ID of an applied protection schedule. explains how to view the IDs of schedules on the system.
Protection schedule paused	Indication of whether an applied protection schedule is currently paused. Value is yes or no.
FAST VP policy	FAST VP policy of the datastore. Value is one of the following: `Start high then auto-tier` `Auto-tier` `Highest available tier` `Lowest available tier`
FAST VP distribution	Percentage of the datastore assigned to each tier. The format is: `<tier_name>:<value>%` where, *‹tier_name›* is the name of the storage tier and *‹value›* is the percentage of storage in that tier.
Local path	Local path to be exported.
Export path	Export path to datastore.
Default access	Default share access settings for host configurations and for unconfigured hosts that can reach the NFS datastore. Value is one of the following: `ro` — Read-only access to primary storage and snapshots associated with the NFS datastore. `rw` — Read/write access to primary storage and snapshots associated with the NFS datastore. `root` — Read/write root access to primary storage and snapshots associated with the NFS datastore. This includes the ability to set access controls that restrict the permissions for other login accounts. `na` — No access to the NFS datastore or its snapshots.

Table **79** NFS datastore attributes (continued)

Attribute	Description
`Read-only hosts`	ID of each host that has read-only permission to the NFS datastore and its snapshots.
`Root hosts`	ID of each host that has root permission to the NFS datastore and its snapshots.
`No access hosts`	ID of each host that has no access to the NFS datastore or its snapshots.
`Deduplication enabled`	Indication of whether deduplication is enabled on the NFS datastore. Valid values are: • `Yes` • `No`
`Creation time`	The time the resource was created.
`Last modified time`	The time the resource was last modified.

Create NFS datastores

Create an NFS datastore.

Prerequisites

- Configure at least one storage pool for the NFS datastore to use and allocate at least one storage disk to the pool. Configure storage pools automatically (physical deployments only) on page 186 explains how to create pools on the system automatically and Configure custom storage pools on page 188 explains how to create custom pools.

- Configure at least one NAS server to which to associate the NFS datastore. Create NAS servers on page 72 explains how to configure NAS servers.

Note

Share access permissions set for specific hosts take effect only if the host-specific setting is less restrictive than the default access setting for the share. Additionally, setting access for a specific host to "No Access" always takes effect over the default access setting.

- Example 1: If the default access setting for a share is Read-Only, setting the access for a specific host configuration to Read/Write will result in an effective host access of Read/Write.

- Example 2: If the default access setting for the share is Read-Only, setting the access permission for a particular host configuration to No Access will take effect and prevent that host from accessing to the share.

- Example 3: If the default access setting for a share is Read-Write, setting the access permission for a particular host configuration to Read-Only will result in an effective host access of Read/Write.

Format

```
/stor/prov/vmware/nfs create [-async] –name <value> [-replDest
{yes|no}] [-descr <value>] -server <value> -pool <value> -size
<value> [-thin {yes|no}][-sched <value> [-schedPaused {yes|
no}]] [-defAccess {ro|rw|root|na}] [-fastvpPolicy
{startHighThenAuto|auto|highest|lowest}][-roHosts <value>] [-
rootHosts <value>] [-naHosts <value>] [-format {UFS32|UFS64}]
```

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.
-name	Type a name for the NFS datastore.
-descr	Type a brief description of the NFS datastore.
-server	Type the ID of the NAS server that will be the primary NAS server for the NFS datastore. View NAS servers on page 74 explains how to view the IDs of the NAS servers on the system.
-pool	Type the name of the storage pool that the NFS datastore will use. **Note** Value is case-insensitive. View storage pools on page 194 explains how to view the names of the storage pools on the system.
-size	Type the quantity of storage to reserve for the NFS datastore. Storage resource size limitations on page 368 explains the limitations on storage size.
-thin	Enable thin provisioning on the NFS datastore. Value is yes or no. Default is no.
-sched	Type the ID of a protection schedule to apply to the storage resource. View protection schedules on page 55 explains how to view the IDs of the schedules on the system.
-schedPaused	Specify whether to pause the protection schedule specified for -sched. Value is yes or no.
-fastvpPolicy	Specify the FAST VP policy of the datastore. Value is one of the following: • startHighThenAuto • auto • highest • lowest
-defAccess	Specify the default share access settings for host configurations and for unconfigured hosts that can reach the NFS datastore. Value is one of the following: • ro — Read-only access to primary storage and snapshots associated with the NFS datastore.

Qualifier	Description
	• `rw` — Read/write access to primary storage and snapshots associated with the NFS datastore. • `root` — Read/write root access to primary storage and snapshots associated with the NFS datastore. This includes the ability to set access controls that restrict the permissions for other login accounts. • `na` — No access to the NFS datastore or its snapshots.
`-roHosts`	Type the ID of each host configuration you want to grant read-only permission to the NFS datastore and its snapshots. Separate each ID with a comma. For host configurations of type 'host,' by default, all of the host's IP addresses can access the NFS datastore and its snapshots. To allow access to only specific IPs, type those specific IPs in square brackets after the host ID. For example: ID[IP,IP], where 'ID' is a host configuration ID and 'IP' is an IP address. View host configurations on page 144 explains how to view the ID of each host configuration.
`-rootHosts`	Type the ID of each host configuration you want to grant root permission to the NFS datastore and its snapshots. Separate each ID with a comma. For host configurations of type 'host,' by default, all of the host's IP addresses can access the NFS datastore and its snapshots. To allow access to only specific IPs, type those specific IPs in square brackets after the host ID. For example: ID[IP,IP], where 'ID' is a host configuration ID and 'IP' is an IP address. View host configurations on page 144 explains how to view the ID of each host configuration.
`-naHosts`	Type the ID of each host configuration you want to block access to the NFS datastore and its snapshots. Separate each ID with a comma. For host configurations of type 'host,' by default, all of the host's IP addresses cannot access the NFS datastore and its snapshots. To limit access for specific IPs, type the IPs in square brackets after the host ID. For example: ID[IP,IP], where 'ID' is a host configuration ID and 'IP' is an IP address. View host configurations on page 144 explains how to view the ID of each host configuration.
`-format`	Datastore format (applies to NFS datastores only). Valid values are: • `UFS32` - Indicates a 32-bit NFS datastore. • `UFS64` - Indicates a 64-bit NFS datastore.

Example

The following command creates an NFS datastore with these settings:

• Named Accounting.

• Description is "Accounting VMs."

• Uses NAS server nas_1 as the primary NAS server.

• Uses the capacity storage pool.

• Primary storage size is 100 GB.

- No protection schedule.

The file system receives the ID NFSDS_1:

**uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/
vmware/nfs create –name Accounting –descr "Accounting VMs" –server
nas_1 –pool capacity –size 100G**

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = NFSDS_1
Operation completed successfully.
```

View NFS datastores

View details about an NFS datastore. You can filter on the NFS datastore ID.

Note

explains how to change the output format.

Format
```
/stor/prov/vmware/nfs [-id <value> [-shrinkToSize <value>]]
show
```

Object qualifier

Qualifier	Description
-id	Identifies the VMware NFS file system.
-shrinkToSize	Specify the targeted shrink size to view an estimate of the minimum size and reclaimable size.
	Note Minimum size and reclaimable size are populated only when this qualifier is specified.

Example 1
The following command lists details about all NFS datastores on the system:

**uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/
vmware/nfs show**

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection


1:      ID                  = NFSDS_1
        Name                = MyVMware
        Description         = My VMware
        Health state        = OK (5)
        Server              = nas_1
        Storage pool ID     = pool_1
        Storage pool        = capacity
        Size                = 536870912000 (500GB)
        Size used           = 128849018880 (120GB)
        Protection size used = 0
```

```
       Local path              = /MyVMware
       Export path             = 10.64.75.10/MyVMware
       Minimum size            =
       Reclaimable size        =
```

Example 2

The following command lists details about the vmware_1 NFS datastores with an shrink estimate:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/

vmware/nfs -id vmware_1 -shrinkToSize 200G show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection


1:     ID                    = vmware_1
       Name                  = MyVMware
       Description           = My VMware
       Health state          = OK (5)
       File system           = fs_1
       Server                = SFServer00
       Storage pool ID       = pool_1
       Storage pool          = capacity
       Format                = UFS64
       Size                  = 536870912000 (500G)
       Size used             = 128849018880 (120G)
       Protection size used  = 0
       Local path            = /
       Export path           = 10.64.75.10/MyVMware
       Minimum size          = 134217728000 (125G)
       Reclaimable size      = 322122547200 (300G)
```

Change NFS datastore settings

Change the settings for an NFS datastore.

Note

Size qualifiers on page 16 explains how to use the size qualifiers when specifying a storage size.

Format
```
/stor/prov/vmware/nfs –id <value> set [-async] –descr <value> -
size <value> [-thin {yes|no}][{-sched <value> | noSched}[-
schedPaused {yes|no}]][-fastvpPolicy {startHighThenAuto|auto|
highest|lowest}][–roHosts <value>] [-rootHosts <value>] [-
naHosts <value>][-replDest {yes | no}]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the NFS datastore to change.

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.
-descr	Type a brief description of the NFS datastore.
-size	Type the amount of storage in the pool to reserve for the NFS datastore. Storage resource size limitations on page 368 explains the limitations on storage size.
-thin	Enable thin provisioning on the NFS datastore. Value is yes or no. Default is no.
-sched	Type the ID of the schedule to apply to the datastore View protection schedules on page 55 explains how to view the IDs of the schedules on the system.
-noSched	Unassigns the protection schedule.
-fastvpPolicy	Specify the FAST VP policy of the datastore. Value is one of the following: • startHighThenAuto • auto • highest • lowest
-schedPaused	Pause the schedule specified for the -sched qualifier. Value is yes or no (default).
-defAccess	Specify the default share access settings for host configurations and for unconfigured hosts who can reach the datastore. Value is one of the following: • ro — Read-only access to primary storage and snapshots associated with the datastore • rw — Read/write access to primary storage and snapshots associated with the datastore. • root — Read/write root access to primary storage and snapshots associated with the datastore. This includes the ability to set access controls that restrict the permissions for other login accounts. • na — No access to the datastore or its snapshots. **Note** Values are case-insensitive.
-roHosts	Type the ID of each host configuration you want to grant read-only permission to the datastore and its snapshots. Separate each ID with a comma. For host configurations of type 'host,' by default, all of the host's IP addresses can access the datastore and its snapshots. To allow access to only specific IPs, type those specific IPs in square brackets after the host ID. For example: ID[IP,IP], where 'ID' is a host configuration ID and 'IP' is an IP address. View

Qualifier	Description
	host configurations on page 144 explains how to view the ID of each host configuration.
-rootHosts	Type the ID of each host configuration you want to grant root permission to the datastore and its snapshots. Separate each ID with a comma. For host configurations of type 'host,' by default, all of the host's IP addresses can access the datastore and its snapshots. To allow access to only specific IPs, type those specific IPs in square brackets after the host ID. For example: ID[IP,IP], where 'ID' is a host configuration ID and 'IP' is an IP address. View host configurations on page 144 explains how to view the ID of each host configuration.
-naHosts	Type the ID of each host configuration you want to block access to the datastore and its snapshots. Separate each ID with a comma. For host configurations of type 'host,' by default, all of the host's IP addresses cannot access the datastore and its snapshots. To limit access for specific IPs, type the IPs in square brackets after the host ID. For example: ID[IP,IP], where 'ID' is a host configuration ID and 'IP' is an IP address. View host configurations on page 144 explains how to view the ID of each host configuration.

Example

The following command changes NFS datastore NFSDS_1 to provide read-only access permissions to host configurations HOST_1 and HOST_2 and blocks access for HOST_3:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/
vmware/nfs –id NFSDS_1 set –roHosts "HOST_1,HOST_2" -naHosts "HOST_3"

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = NFSDS_1
Operation completed successfully.
```

Delete NFS datastores

Delete an NFS datastore.

Note

Deleting an NFS datastore removes any files and folders associated with it from the system. You cannot use snapshots to restore the contents of the datastore. Back up the data from the datastore before deleting it from the system.

Format

```
/stor/prov/vmware/nfs -id <value> delete [-async]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the NFS datastore to delete.

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.

Example

The following command deletes NFS datastore NFSDS_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/
vmware/nfs -id NFSDS_1 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage VMware VMFS datastores

Virtual Machine Filesystem (VMFS) datastores provide block storage for ESX Server hosts. VMFS datastores appear to ESX Server hosts as LUNs, to which the hosts connect through the iSCSI protocol. You can provision and manage NFS datastores and view details about each NFS datastore on the system, such as their storage capacity and health.

Each VMFS datastore is identified by an ID.

The following table lists the attributes for VMFS datastores.

Table 80 VMFS datastore attributes

Attribute	Description
ID	ID of the VMFS datastore.
LUN	Logical unit number (LUN) ID of the VMFS datastore.
Name	Name of the VMFS datastore.
Description	Brief description of the VMFS datastore.
Health state	Health state of the VMFS datastore. The health state code appears in parentheses. Value is one of the following: • OK (5) — VMFS datastore is operating normally. • Degraded/Warning (10) — Working, but one or more of the following may have occurred: ■ One or more of its storage pools are degraded. ■ Its replication session is degraded. ■ Its replication session has faulted. ■ It has almost reached full capacity. Increase the primary storage size, or create additional datastores to store your data, to avoid data loss. Change VMware VMFS datastore settings on page 269 explains how to change the primary storage size. • Minor failure (15) — One or both of the following may have occurred:

Table 80 VMFS datastore attributes (continued)

Attribute	Description
	■ One or more of its storage pools have failed.
	■ The associated iSCSI node has failed.
	• `Major failure (20)` — One or both of the following may have occurred:
	■ Datastore is unavailable.
	■ One or more of the associated storage pools have failed.
	• `Critical failure (25)` — One or more of the following may have occurred:
	■ One or more of its storage pools are unavailable.
	■ Datastore is unavailable.
	■ Datastore has reached full capacity. Increase the primary storage size, or create additional file systems to store your data, to avoid data loss. Change VMware VMFS datastore settings on page 269 explains how to change the primary storage size.
	• `Non-recoverable error (30)` — One or both of the following may have occurred:
	■ One or more of its storage pools are unavailable.
	■ Datastore is unavailable.
`Health details`	Additional health information. See Appendix A, Reference, for health information details.
`Storage pool ID`	ID of the storage pool the datastore uses.
`Storage pool`	Name of the storage pool the LUN is using.
`Size`	Quantity of storage reserved for primary data.
`Maximum size`	Maximum size to which you can increase the primary storage capacity.
`Thin provisioning enabled`	Indication of whether thin provisioning is enabled. Value is yes or no. Default is no. All storage pools support both standard and thin provisioned storage resources. For standard storage resources, the entire requested size is allocated from the pool when the resource is created, for thin provisioned storage resources only incremental portions of the size are allocated based on usage. Because thin provisioned storage resources can subscribe to more storage than is actually allocated to them, storage pools can be over provisioned to support more storage capacity than they actually possess.
	Note
	The Unisphere online help provides more details on thin provisioning.
`Current allocation`	If thin provisioning is enabled, the quantity of primary storage currently allocated through thin provisioning.
`Protection size used`	Quantity of storage currently used for protection data.

Table 80 VMFS datastore attributes (continued)

Attribute	Description
Snapshot count	Total number of snapshots on the datastore.
Maximum protection size	Maximum size to which you can increase the protection storage size.
Protection schedule	ID of a protection schedule applied to the VMFS datastore . View protection schedules on page 55 explains how to view the IDs of the schedules on the system.
Protection schedule paused	Indication of whether an applied protection schedule is currently paused.
Snapshot auto-delete	Indicates whether application snapshots can be deleted automatically. Value is one of the following: • Yes • No
SP owner	Indicates the default owner of the LUN. Value is one of the following: • SP A • SP B
Trespassed	Indicates whether the LUN is trespassed to the peer SP. Value is one of the following: • Yes • No
LUN access hosts	List of hosts with access permissions to the VMFS datastore, presented to the hosts as a LUN.
Snapshots access hosts	List of hosts with access permissions to the VMFS datastore snapshots.
WWN	World Wide Name of the VMware resource.
Replication destination	Flag indicating whether the resource is a destination for a replication session. Value is one of the following: • Yes • No
Creation time	The time the resource was created.
Last modified time	The time the resource was last modified.
FAST VP policy	FAST VP policy of the datastore. Value is one of the following: • Start high then auto-tier • Auto-tier • Highest available tier • Lowest available tier

Attribute	Description
`FAST VP distribution`	Percentage of the datastore assigned to each tier. The format is: `<tier_name>:<value>%` where, *‹tier_name›* is the name of the storage tier and *‹value›* is the percentage of storage in that tier.
`Version`	Indicates the VMFS version of the datastore. Value is one of the following: • 3 • 5
`Block size`	Indicates the block size in megabytes. Value is one of the following: • 1 • 2 • 4 • 8

Create VMware VMFS datastores

Create a VMFS datastore.

Prerequisites

• Configure at least one storage pool for the VMFS datastore to use and allocate at least one storage disk to the pool. Configure storage pools automatically (physical deployments only) on page 186 explains how to create pools on the system automatically and Configure custom storage pools on page 188 explains how to create custom pools.

• Configure at least one iSCSI node to which to associate the VMFS datastore. View iSCSI nodes on page 95 explains how to create iSCSI nodes on the system.

Format
```
/stor/prov/vmware/vmfs create [-async] -name <value> [-descr
<value>] pool <value> -size <value> [-thin {yes | no}] [-sched
<value> [-schedPaused {yes | no}]] [-fastvpPolicy
{ startHighThenAuto | auto | highest | lowest }] [-vdiskHosts
<value>] [-snapHosts <value>] [-replDest {yes | no}] [-version
{3 [-blockSize {1 | 2 | 4 | 8}] | 5}]
```

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-name`	Type a name for the VMFS datastore.

Qualifier	Description
	Note Use a name that reflects the type and version of the application that will use it, which can facilitate how the VMFS datastore is managed and monitored through Unisphere.
-descr	Type a brief description of the VMFS datastore.
-pool	Type the name of the storage pool that the VMFS datastore will use. **Note** Value is case-insensitive. View storage pools on page 194 explains how to view the names of the storage pools on the system.
-size	Type the quantity of storage to reserve for the VMFS datastore. Storage resource size limitations on page 368 explains the limitations on storage size.
-thin	Enable thin provisioning on the VMFS datastore. Value is yes or no. Default is no.
-sched	Type the ID of a protection schedule to apply to the storage resource. View protection schedules on page 55 explains how to view the IDs of the schedules on the system.
-schedPaused	Specify whether to pause the protection schedule specified for -sched. Value is yes or no.
-vdiskHosts	Type the ID of each host configuration to give access to the VMFS datastore. Separate each ID with a comma. By default, all iSCSI initiators on the host can access the VMFS datastore. To allow access for specific initiators, type the IQN of each initiator in square brackets after the host ID. For example: ID[IQN,IQN], where 'ID' is a host configuration ID and 'IQN' is an initiator IQN. View host configurations on page 144 explains how to view the ID of each host configuration.
-snapHosts	Type the ID of each host configuration to give access to snapshots of the VMFS datastore. Separate each ID with a comma. By default, all iSCSI initiators on the host can access all VMFS datastore snapshots. To allow access for specific initiators, type the IQN of each initiator in square brackets after the host ID. For example: ID[IQN,IQN], where 'ID' is a host configuration ID and 'IQN' is an initiator IQN. View host configurations on page 144 explains how to view the ID of each host configuration.
-replDest	Specifies whether the resource is a replication destination. Valid values are: • Yes • No (default)

Qualifier	Description
	Note Values are case insensitive.
-fastvpPolicy	Specify the FAST VP policy of the datastore. Value is one of the following: • startHighThenAuto • auto • highest • lowest
-version	Type the VMFS version of the datastore. Value is one of the following: • 3 (default) • 5
-blockSize	Type the block size in megabytes of the datastore. Value is one of the following: • 1 • 2 • 4 • 8 (default)

Example

The following command creates a VMFS datastore with these settings:

- Name is Accounting3.
- Description is "Accounting Group 3."
- Uses the capacity storage pool.
- Provides host access permissions to the VMFS datastore (presented as a LUN) to two of the IQNs for host configuration 1014 and for host configuration 1015.
- No protection schedule.

The VMFS datastore receives the ID VMFS_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/
vmfs create –name "Accounting3" –descr "Accounting Group 3" –pool
capacity -size 100G –thin yes –vdiskHosts "1014,1015"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = VMFS_1
Operation completed successfully.
```

View VMware VMFS datastores

Display the list of existing VMFS datastores. You can filter on the ID of a VMFS datastore.

Note

explains how to change the output format.

Format

```
/stor/prov/vmware/vmfs [-id <value>] show
```

Object qualifier

Qualifier	Description
-id	Type the ID of a VMFS datastore.

Example

The following command displays details about the VMFS datastore on the system:

**uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/
vmfs show**

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID                  = VMFS_1
        LUN                 = sv_1
        Name                = MyVMware
        Description         = My description
        Health state        = OK (5)
        Storage pool ID     = pool_2
        Storage pool        = capacity
        Size                = 107374182400 (100G)
        Protection size used = 0
        SP owner            = SPA
        Trespassed          = no
```

Change VMware VMFS datastore settings

Change the settings for a VMFS datastore.

Format

```
/stor/prov/vmware/vmfs -id <value> set [-async] [-name <value>]
[-descr <value>] [-size <value>] [{-sched <value> | -noSched}]
[-schedPaused {yes | no}] [-vdiskHosts <value>] [-snapHosts
<value>] [-spOwner {spa | spb}] [-fastvpPolicy
{ startHighThenAuto | auto | highest | lowest | none}] [-
replDest {yes | no}]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the VMFS datastore to change.

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.
-name	Type a name for the VMFS datastore.

Qualifier	Description
	Note Use a name that reflects the type and version of the application that will use it, which can facilitate how the VMFS datastore is managed and monitored through Unisphere.
-descr	Type a brief description of the VMFS datastore.
-size	Type the quantity of storage to allocate for the VMFS datastore. Storage resource size limitations on page 368 explains the limitations on storage size.
-sched	Type the ID of a protection schedule to apply to the VMFS datastore. View protection schedules on page 55 explains how to view the IDs of the schedules on the system.
-schedPaused	Specify whether to pause the protection schedule specified for -sched. Value is yes or no.
-noSched	Unassign the protection schedule.
-vdiskHosts	Type the ID of each host configuration to give access to the VMFS datastore. Separate each ID with a comma. By default, all iSCSI initiators on the host can access the VMFS datastore. To allow access for specific initiators, type the IQN of each initiator in square brackets after the host ID. For example: ID[IQN,IQN], where 'ID' is a host configuration ID and 'IQN' is an initiator IQN. View host configurations on page 144 explains how to view the ID of each host configuration.
-snapHosts	Type the ID of each host configuration to give access to snapshots of the VMFS datastore. Separate each ID with a comma. By default, all iSCSI initiators on the host can access all VMFS datastore snapshots. To allow access for specific initiators, type the IQN of each initiator in square brackets after the host ID. For example: ID[IQN,IQN], where 'ID' is a host configuration ID and 'IQN' is an initiator IQN. View host configurations on page 144 explains how to view the ID of each host configuration.
-spOwner	Specify the default SP that owns the datastore.
-replDest	Specifies whether the resource is a replication destination. Valid values are: • yes • no **Note** Values are case insensitive.
-fastvpPolicy	Specify the FAST VP policy of the datastore. Value is one of the following: • startHighThenAuto • auto • highest

Qualifier	Description
	• `lowest`

Example

The following command updates VMFS datastore VMFS_1 with these settings:

- Name is Accounting4.

- Description is "Accounting Group 4."

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/
vmfs –id VMFS_1 set –name Accounting4 –descr "Accounting Group 4"

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = VMFS_1
Operation completed successfully.
```

Delete VMware VMFS datastores

Delete a VMFS datastore.

Deleting a VMFS datastore removes all data and snapshots of it from the system. After the VMFS datastore is deleted, you cannot restore the data from snapshots. Back up all data from the VMFS datastore before deleting it.

Format
```
/stor/prov/vmware/vmfs –id <value> delete [-deleteSnapshots
{yes | no}] [-async]
```

Object qualifier

Qualifier	Description
`–id`	Type the ID of the VMFS datastore to delete.

Action qualifier

Qualifier	Description
`–async`	Run the operation in asynchronous mode.
`–deleteSnapshots`	Specify whether the datastore can be deleted along with snapshots. Value is Yes or No (default).

Example

The following command deletes VMFS datastore VMFS_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/
vmfs –id VMFS_1 delete

```
Storage system address: 10.0.0.1
Storage system port: 443
```

```
HTTPS connection

Operation completed successfully.
```

Manage data deduplication

Deduplication increases file storage efficiency by eliminating redundant data from the files stored in the file system on a storage resource, such as a file system, which saves storage space. Enable deduplication on a storage resource and the system scans the filesystem on the storage resource for redundant data and deduplicates the data to free storage space. The scan runs once every week.

When the system is busy, scanning is limited, or suspended, so as not to further reduce system performance. When the system returns to normal operation, normal scanning resumes. After deduplicating a filesystem, the amount of storage used by the storage resource is significantly reduced, as much as 50 percent. The Unisphere online help provides more details about deduplication.

You can enable deduplication for file systems.

This command supports asynchronous execution.

The following table lists the attributes for deduplication:

Table 81 Deduplication attributes

Attribute	Description
ID	ID of the storage resource on which deduplication is enabled.
Enabled	Indication of whether deduplication is enabled. Value is yes or no.
State	State of deduplication, which performs a scan once a week. Value is one of the following: • paused — System is not currently scanning the storage resource. • running — System is currently scanning the storage resource. This is the default value when deduplication is enabled.
Excluded file extensions	List of file extensions that specify the files that will not be deduplicated. Each file extension is separated by a colon.
Excluded paths	List of paths on the filesystem that contains files that will not be deduplicated. Each path is separated by a semi-colon.
Last scan	Date and time when the system last scanned the filesystem.
Files deduplicated	The number and percentages of files deduplicated. Value appears in the <num>(<perc>%) format. Where: • *num* - Number of files deduplicated. • *perc* % - Percentage of files deduplicated.
Percent complete	Status (as a percentage) of the deduplication scan process.
Total size	Total capacity size of the storage resource on which deduplication is enabled.
Original size used	Amount of storage used by the storage resource before its files are deduplicated.

Table 81 Deduplication attributes (continued)

Attribute	Description
`Current size used`	Amount of storage used by the storage resource after its files are deduplicated.

View deduplication settings

View details about the deduplication settings on the system.

Note

explains how to change the output format.

Format
```
/eff/dedup [-id <value>] show
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of a storage resource on which deduplication is enabled.

Example
The following command displays the deduplication settings:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /eff/dedup show`

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
1:      ID                = SFS_1
        Resource type     = sf
        State             = running
        File exclude list = .jpg:.gif
        Path exclude list = /home/photo
        Last scan         = 2014-04-25 04:42:28
        Files deduplicated = 10 (30%)
        Percent complete  = 100%
        Total size        = 2147483648 (2.0G)
        Original size used = 8192 (8.0K)
        Current size used = 2818048 (2.6M)
```

Configure deduplication settings

Configure deduplication settings for a storage resource.

Format
```
/eff/dedup -id <value> set [-async] [-enabled {yes|no}] [-state
{running|paused}] [-fileExcList <value>] [-pathExcList <value>]
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the storage resource on which to configure deduplication.

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.
-enabled	Enable deduplication. Valid values are: • Yes • No **Note** When you disable deduplication, all files on the storage resource will be re-deduplicated, which returns the storage usage to its original size before the files were deduplicated. Ensure the storage pool can accommodate the added storage use before disabling deduplication.
-state	Specify to pause or run deduplication scanning, which scans the target storage resource once a week. Value is one of the following: • running — System will scan the storage resource. This is the default value when -enabled is yes. • paused — System will not scan the storage resource. **Note** To change this qualifier, deduplication must be enabled.
-fileExcList	Type a list of file extensions for files that will not be deduplicated. Use a semicolon to separate each file extension. **Note** To change this qualifier, deduplication must be enabled and -state must be paused.
-pathExcList	List of paths on the file system that contain files that will not be deduplicated. Use a colon to separate the paths. **Note** To change this qualifier, deduplication must be enabled and -state must be paused.

Example

The following command pauses deduplication scanning for file system fs_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /eff/dedup -id fs_1
set -state paused
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = nas_1
Operation completed successfully.
```

Force a rescan

Rescan a target storage resource to deduplicate it immediately. By default, the system performs a scan once every week.

Format
```
/eff/dedup -id <value> rescan -async
```

Object qualifier

Qualifier	Description
-id	Type the ID of a storage resource on which deduplication is enabled.

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.

Example
The following command forces deduplication scanning of file system fs_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /eff/dedup -id fs_1 rescan

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

CHAPTER 7

Protect Data

This chapter addresses the following topics:

Manage snapshots

A snapshot is a virtual point-in-time image of the data within a storage resource that has changed since the last snapshot. Snapshots provide a record of the content in the targeted storage resource at a particular date and time, but are not mirror copies of the data. Periodically creating snapshots of file systems and LUNs provides an effective technique for meeting data protection and recovery requirements. Based on the importance and volatility of data within a storage resource, you can define recurring schedules that specify times and intervals for snapshot operations.

Use snapshots to perform the following:

- Restore a storage resource to a previous point-in-time.

- Access the contents of a snapshot to recover corrupted or accidentally deleted files and data.

To routinely take snapshots automatically, associate a snapshot with a schedule. Manage snapshot protection schedules on page 55 explains how to configure schedules on the system. Each snapshot is identified by an ID.

Note

Snapshots do not provide a substitute for storage backup operations. Snapshots are not intended to provide resources for recovering from disasters or the loss of physical equipment.

Note

To ensure a host has the correct permissions to access snapshots, check the host access permissions for the appropriate storage resource. View file systems on page 223 explains how to view host access permissions for file systems. View LUN groups on page 250 explains how to view the host access permissions for iSCSI storage resources.

The following table lists the attributes for snapshots:

Table 82 Snapshot attributes

Attribute	Description
ID	ID of the snapshot.
Name	Name of the snapshot.
State	State of the snapshot. Value is one of the following: - `OK` - Snapshot is available to hosts. - `Expired` - Snapshot has expired. The system will delete it automatically.
Attached	Indicates whether the snapshot is attached to a storage resource. **Note** This field is blank for file system snapshots.
Source	ID of the storage resource of which the system created the snapshot.
Source type	Type of storage resource of which the system created the snapshot.

Table 82 Snapshot attributes (continued)

Attribute	Description
`Attach details`	Comma-separated list of export paths or WWNs for promoted snapshots.
`Members`	Comma-separated list of the member LUNs of the snapshot. **Note** This field is blank for file system snapshots.
`Source snapshot`	For a snapshot of a snapshot, the ID of the parent snapshot.
`Description`	Snapshot description.
`Creation time`	Date and time when the snapshot was created.
`Expiration time`	Date and time when the snapshot will expire and be deleted from the system. Default is 7 days.
`Last writable time`	Last time the snapshot or its parent snapshot was detached.
`Created by`	Name of the user, protection schedule, or backup process that created the snapshot. Value is one of the following: • For manual snapshots created by a user, the user account name. • For scheduled snapshots, the name of the protection schedule. • For snapshots created by host backup software: ■ `NDMP` - Indicates a snapshot created by using the Network Data Management Protocol (NDMP). ■ `VSS` - Indicates a snapshot created by using the Microsoft Volume Snapshot Service (VSS), also called Shadow Copy or Previous Version. • `Snapshot Restore` - Indicates a snapshot created automatically by the system when restoring a file system or VMware NFS datastore. You can use the snapshot to return the storage resource to the state it was in prior to the last restore.
`Modified`	Indicates whether the snapshot is or was previously attached to a snapshot mount point, or has shares. Value is one of the following: • `Yes` • `No`
`Allow auto-delete`	Indicates whether or not the system can automatically delete the snapshot. Value is one of the following: • `Yes` • `No` Default value is `yes`.
`Size`	Pool capacity consumed by the snapshot.

Table 82 Snapshot attributes (continued)

Attribute	Description
	Note This field is blank for snapshots of LUN groups and VMware block applications.
Access	Indicates whether a file system snapshot is a read-only checkpoint, or read/write for user access.

Create snapshots

Create a snapshot of a storage resource.

Note

Snapshots of LUNs are not intended for use as mirrors, disaster recovery, or high-availability tools. Because LUN snapshots are partially derived from real-time data on the LUNs, snapshots can become inaccessible (not readable) if the primary LUN becomes inaccessible.

Prerequisites

Snapshots are stored in the protection capacity of the storage resource. Ensure that enough protection capacity exists to accommodate snapshots. View file systems on page 223 explains how to view the current protection storage size for file systems. View LUNs on page 244 explains how to view the current protection size for iSCSI storage resources.

Format
```
/prot/snap create [-async] [-name <value>] [-descr <value>] [{-
keepFor <value>| -allowAutoDelete {yes|no}}] [-access {ckpt |
share} ]
```

Action qualifiers

Qualifier	Description
-async	Run the operation in asynchronous mode.
-name	Type a name for the snapshot.
-descr	Type a description for the snapshot.
-source	Type the ID of the storage resource of which to take a snapshot. View file systems on page 223 explains how to view the settings for file systems. View LUN groups on page 250 explains how to view the settings for iSCSI storage resources
-keepFor	Type the number of days or hours to retain a snapshot before it expires. The system deletes expired snapshots automatically. Use the following format: *<value><qualifier>* where:

Qualifier	Description

	• `value` — Type the number of hours or days:
	   ▪ For hours, the range is 1–744.
	   ▪ For days, the range is 1–31.
	 • `qualifier` — Type the value qualifier. Value is one of the following:
	   ▪ `h` — Indicates hours.
	   ▪ `d` — Indicates days.
	 Default value is 7d (7 days).
	
	 Note
	
	 For scheduled snapshots, which are associated with a schedule, include the `-keepFor` qualifier in the schedule rules to specify the retention period. Manage task rules on page 56 provides details about schedule rules.

`-allowAutoDelete`	Specify whether the system can automatically delete the snapshot or snapshot set. Use the following format: `<value>` where *value* is **yes** or **no**. Default value is **yes**.
`-access`	Specify whether the snapshot is a read-only checkpoint, or read/write for CIFS shares or NFS exports. Use the following format: `<value>` where value is **ckpt** or **share**. Default value is **ckpt**.

Example

The following command takes a snapshot of a file system with these settings:

- Name is accounting.
- Storage resource is file system FS_1.
- Retention period is 1 day.

The snapshot receives ID SNAP_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap create –
name accounting –source FS_1 -keepFor 1d
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = SNAP_1
Operation completed successfully.
```

View snapshots

View details about snapshots on the system. You can filter on the snapshot ID, snapshot name, or storage resource ID.

Note

The show action command on page 17 explains how to change the output format.

Format

```
/prot/snap [{-id <value> | -name <value> | -source <value>}]
show
```

Object qualifier

Qualifier	Description
-id	Type the ID of a snapshot.
-name	Type the name of the snapshot.
-source	Type the ID of a storage resource to view only the snapshots related to it.

Example

The following command displays details about all snapshots on the system:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection


1:      ID                = SNAP_1
        Name              = Snapshot1
        State             = OK
        Attached          = no
        Resource          = app_1
        Resource type     = LUN group
        Source            = app_1
        Source type       = LUN group
        Members           = sv_1,sv_2
        Attach details    = 60:06:01:60:D2:04:00:00:78:4F:09:51:22:EB:
34:E3, 60:06:01:60:D2:04:00:00:78:4F:09:51:22:EB:34:E4

2:      ID                = SNAP_2
        Name              = Snapshot2
        State             = OK
        Attached          = no
        Resource          = app_1
        Resource type     = LUN group
        Source            = app_2
        Source type       = LUN group
        Members           = sv_3,sv_4
        Attach details    = 60:06:01:60:D2:04:00:00:78:4F:09:51:22:EB:
34:E3, 60:06:01:60:D2:04:00:00:78:4F:09:51:22:EB:34:E4
```

Attach snapshots to hosts

For snapshots of storage resources, attach a snapshot to make it available to hosts.

Note

Before a host can access an attached snapshot, it must have snapshot permissions to the appropriate storage resource. Manage LUNs on page 240 explains how to configure host access permissions for LUN storage resources.

Format
```
/prot/snap { -id <value> | -name <value> } attach [ -async ]
[ -copyName <value> ]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the snapshot to promote.
-name	Type the name of the snapshot to attach.

Action qualifiers

Qualifier	Description
-async	Run the operation in asynchronous mode.
-copyName	Type the name of the copy the system creates before attaching the selected snapshot. If this switch is specified and no name is provided, the system assigns a name to the copy. **Note** If this switch is not specified, no copy is created.

Example
The following command promotes snapshot SNAP_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap –id

SNAP_1 attach

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = SNAP_1
Operation completed successfully.
```

Detach snapshots

For snapshots of storage resources, detach an attached snapshot to block host access to the snapshot.

Note

Before a host can access an attached snapshot, it must have snapshot permissions to the appropriate storage resource. Manage LUNs on page 240 explains how to configure host access permissions for LUN storage.

Format
```
/prot/snap {-id <value> | -name <value> } detach [-async]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the snapshot to detach.

Qualifier	Description
-name	Type the name of the snapshot to detach.

Action qualifiers

Qualifier	Description
-async	Run the operation in asynchronous mode.

Example

The following command detaches snapshot SNAP_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap -id
SNAP_1 detach
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Restore storage resources to snapshots

Restore a storage resource to a snapshot to return (roll back) the storage resource to a previous state. During the restore, the entire storage resource, including all files and data stored on it, is replaced with the contents of the selected snapshot.

Note

Before the restoration begins, the system creates a snapshot of the file system to be restored. You can use the snapshot to restore the file system to its previous state before you restored it the first time.

Note

For LUNs, any snapshots that were created after the snapshot to which you restore are destroyed and cannot be recovered. For file systems, all snapshots remain on the system.

Prerequisites

- To prevent data loss, ensure that all hosts have completed all read and write operations to the storage resource you want to restore.

- For LUN storage:

  - If the snapshot is promoted you must first demote it or an error will appear when you attempt to restore to it.

  - If a host is connected to the LUN (seen by the host as a disk) you want to restore, the restore will not complete. Perform one of the following to the LUN to disconnect it from the host:

    - On Windows, disable the LUN in the Device Manager, which might require a host reboot.

    - On Linux/UNIX, run the unmount command on the virtual.

    Once the LUN is disconnected, you can continue with the restore and then enable and mount the restored LUN on the host.

Format
```
/prot/snap {-id <value> | -name <value> } restore [-backupName
<value>][-async]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the snapshot to which you want to restore the associated storage resource.
-name	Type the name of the snapshot to which you want to restore the associated storage resources.

Action qualifiers

Qualifier	Description
-async	Run the operation in asynchronous mode.
-backupName	Specifies the name of the snapshot the system creates automatically as the initial step of the restoration process. The system assigns a name to this snapshot if the user does not provide one.

Example
The following command restores snapshot SNAP_1, which is a snapshot of iSCSI storage:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap -id SNAP_1 restore

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Delete snapshots

Delete (destroy) a snapshot of a storage resource.

Note

Once you delete a snapshot, you can no longer recover data from it or restore a storage resource to it.

Format
```
/prot/snap { -id <value> | -name <value> } delete [-async]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the snapshot to promote.
-name	Type the name of the snapshot.

Action qualifiers

Qualifier	Description
-async	Run the operation in asynchronous mode.

Example

The following command deletes snapshot SNAP_1:

**uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap –id
SNAP_1 delete**

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Copy snapshots

Copy a snapshot.

Format
```
/prot/snap { -id <value> | -name <value> } copy [-async] [-
copyName <value>]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the snapshot to which you want to restore the associated storage resource.
-name	Type the name of the snapshot to which you want to restore the associated storage resources.

Action qualifiers

Qualifier	Description
-async	Run the operation in asynchronous mode.
-copyName	Type the name of the copy the system creates before attaching the selected snapshot. If this switch is specified and no name is provided, the system assigns a name to the copy. **Note** If this switch is not specified, no copy is created.

Example

The following command creates a copy of SNAP_1 named SNAP_Copy:

• Name is accounting.

The snapshot receives ID SNAP_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap -id
SNAP_1 copy -copyName SNAP_Copy
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = SNAP_1
Operation completed successfully.
```

Modify snapshots

Change the settings of a snapshot.

Format

```
/prot/snap { -id <value> | -name <value> } set [-async] [-
newName <value>] [-descr <value>] [{-keepFor <value> | -
allowAutoDelete {yes|no}}]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the snapshot to which you want to restore the associated storage resource.
-name	Type the name of the snapshot to which you want to restore the associated storage resources.

Action qualifiers

Qualifier	Description
-async	Run the operation in asynchronous mode.
-newName	Type a new name for the snapshot.
-descr	Type a description for the snapshot.
-keepFor	Type the number of days or hours to retain a snapshot before it expires. The system deletes expired snapshots automatically. Use the following format: *<value><qualifier>* where: • value — Type the number of hours or days: ▪ For hours, the range is 1–744. ▪ For days, the range is 1–31. • qualifier — Type the value qualifier. Value is one of the following: ▪ h — Indicates hours. ▪ d — Indicates days. Default value is 7d (7 days).

Qualifier	Description
	Note For scheduled snapshots, which are associated with a schedule, include the `-keepFor` qualifier in the schedule rules to specify the retention period. Manage task rules on page 56 provides details about schedule rules.
`-allowAutoDelete`	Specify whether the system can automatically delete the snapshot or snapshot set. Use the following format: `<value>` where *value* is **yes** or **no**. Default value is **yes**.

Example

The following command changes the name of snapshot SNAP_1 to MySnap:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap -id
SNAP_1 set -newName MySnap

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = SNAP_1
Operation completed successfully.
```

Manage snapshot NFS shares

The following table lists the attributes for snapshot NFS share:

Table 83 Snapshot NFS share attributes

Attribute	Description
`ID`	ID of the snapshot NFS share.
`Name`	Name of the snapshot NFS share.
`Description`	Description of the snapshot NFS share.
`Snapshot`	Parent snapshot (see Manage snapshots on page 278.)
`Local path`	Local path to be exported.
`Export path`	Export path to the share.
`Default access`	Specifies the default access level. Valid values are: • `ro` — Read-only access • `rw` — Read/Write access • `root` — Root access • `na` — No access

Table 83 Snapshot NFS share attributes (continued)

Attribute	Description
	Note Values are case insensitive.
Read-only hosts	Comma-separated list of identifiers of hosts allowed reading data.
Read/write hosts	Comma-separated list of identifiers of hosts allowed reading and writing data.
Root hosts	Comma-separated list of identifiers of hosts with root permissions.
No access hosts	Comma-separated list of identifiers of hosts without access.
Creation time	Creation time of the share.
Last modified time	Last modified time of the share.

Note

`Read-only hosts`, `Read/write hosts`, `Root hosts`, and `No access hosts` attributes are displayed as a comma-separated list of pairs of host identifiers and tokens enclosed with square brackets. The token format depends on the host type:

- host — Comma-separated list of IP addresses.
- subnet — Pair of IP address and netmask delimited by slash.
- netgroup — Netgroup network address.

Create NFS snapshots

Create a snapshot NFS share.

Format
```
/prot/snap/nfs create [-async] -name <value> [-descr <value>] -
snap <value> -path <value> [-defAccess {ro | rw | root | na}]
[-roHosts <value>] [-rwHosts <value>] [-rootHosts <value>] [-
naHosts <value>]
```

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.
-name	Type the username of the share.
-descr	Type the description of the share.
-snap	Type the snapshot to associate the share with.
-path	Type the path at which to mount the file system. Default value is /.
-defAccess	Specifies the new user description of the share. Value is one of the following: - `ro` — Read-only access

Qualifier	Description
	• `rw` — Read/Write access • `root` — Root access • `na` — No access **Note** Values are case insensitive.
`-roHosts`	Specifies the comma-separated list of identifiers of hosts allowed to read. Optionally, it's allowed to select the IP addresses of the host of type host. They shall be defined as a comma-separated list of IP addresses enclosed with square brackets and following the host identifier.
`-rwHosts`	Specifies the comma-separated list of identifiers of hosts allowed to read and write. Optionally, it's allowed to select the IP addresses of the host of type host. They shall be defined as a comma-separated list of IP addresses enclosed with square brackets and following the host identifier.
`-rootHosts`	Specifies the comma-separated list of identifiers of hosts with root permissions. Optionally, it's allowed to select the IP addresses of the host of type host. They shall be defined as a comma-separated list of IP addresses enclosed with square brackets and following the host identifier.
`-naHosts`	Specifies the comma-separated list of identifiers of hosts without access. Optionally, it's allowed to select the IP addresses of the host of type host. They shall be defined as a comma-separated list of IP addresses enclosed with square brackets and following the host identifier.

Example

The following command takes a snapshot of a file system with these settings:

• Name is NFSshare.

• Description is "My share."

• Snapshot ID is SNAP_1.

• Path is /.

• Read-only hosts are Host_1 and Host_2.

• Read/write host is Host_3.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap/nfs
create —name NFSshare -descr "My share" —snap SNAP_1 -path / -roHosts
"Host_1, Host_2" -rwHosts "Host_3"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = nfs_1
Operation completed successfully.
```

View snapshot NFS shares

Lists the existing snapshot NFS shares.

Format

```
/prot/snap/nfs [{-id <value> | -snap <value>}] show
```

Object qualifier

Qualifier	Description
-id	Identifies the NFS share.
-snap	Identifies the parent snapshot. The list of shares associated with the identified snapshot will be displayed.

Example

uemcli /prot/snap/nfs show -detail

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:    ID                 = nfs_2
      Name               = Share_2012-08-24 16:05_00
      Description        =
      Snapshot           = app_1_sg_1
      Local path         = /group.app_1_sg_1.fs.fs_1_wckp
      Export path        = 10.64.76.120:/Share_2012-08-24 16:05_00
      Default access     = na
      No access hosts    =
      Read-only hosts    = 1014[10.192.168.5,10.192.168.6],
1015[10.192.168.9]
      Read/write hosts   = 1016[10.244.245.0/255.255.255.0]
      Root hosts         =
      Creation time      = 2012-08-24 12:18:22
      Last modified time = 2012-08-24 12:18:22
```

Set snapshot NFS share

Modifies an existing snapshot NFS share.

Format

```
/prot/snap/nfs -id <value> set [-async] [-descr <value>] [-
defAccess { ro | rw | root | na }] [ -roHosts <value>] [-
rwHosts <value>] [-rootHosts <value>] [-naHosts <value>]
```

Object qualifier

Qualifier	Description
-id	Identifies the snapshot NFS share.

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.
-descr	Type the description of the share.

Qualifier	Description
-defAccess	Specifies the new user description of the share. Value is one of the following: • `ro` — Read-only access • `rw` — Read/Write access • `root` — Root access • `na` — No access **Note** Values are case insensitive.
-roHosts	Specifies the comma-separated list of identifiers of hosts allowed to read. Optionally, it's allowed to select the IP addresses of the host of type host. They shall be defined as a comma-separated list of IP addresses enclosed with square brackets and following the host identifier.
-rwHosts	Specifies the comma-separated list of identifiers of hosts allowed to read and write. Optionally, it's allowed to select the IP addresses of the host of type host. They shall be defined as a comma-separated list of IP addresses enclosed with square brackets and following the host identifier.
-rootHosts	Specifies the comma-separated list of identifiers of hosts with root permissions. Optionally, it's allowed to select the IP addresses of the host of type host. They shall be defined as a comma-separated list of IP addresses enclosed with square brackets and following the host identifier.
-naHosts	Specifies the comma-separated list of identifiers of hosts without access. Optionally, it's allowed to select the IP addresses of the host of type host. They shall be defined as a comma-separated list of IP addresses enclosed with square brackets and following the host identifier.

Example

```
uemcli /stor/prov/sf/nfs -id NFS_1 set -descr "My share"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = NFS_1
Operation completed successfully.
```

Delete snapshot NFS shares

Delete (destroy) a snapshot NFS share.

Note

Once you delete a snapshot, you can no longer recover data from it or restore a storage resource to it.

Format

```
/prot/snap/nfs –id <value> delete [-async]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the snapshot to delete.

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.

Example

The following command deletes snapshot nfs_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap/nfs –id nfs_1 delete

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage snapshot CIFS shares

The following table lists the attributes for snapshot CIFS shares.

Table 84 Snapshot CIFS share attributes

Attribute	Description
ID	ID of the snapshot CIFS share.
Name	Name of the snapshot CIFS share.
Description	Description of the snapshot CIFS share.
Snapshot	Parent snapshot (see Manage snapshots on page 278.)
Local path	Local path to be exported.
Export path	Export path to the share.
Creation time	Creation time of the share.
Last modified time	Last modified time of the share.
Availability enabled	Continuous availability state.
Encryption enabled	CIFS encryption state.
Umask	Indicates the default Unix umask for new files created on the share. If not specified, the umask defaults to 022.

Table 84 Snapshot CIFS share attributes (continued)

Attribute	Description
ABE enabled	Indicates whether an Access-Based Enumeration (ABE) filter is enabled. Valid values include: • yes — Filters the list of available files and folders on a share to include only those that the requesting user has access to. • no (default)
DFS enabled	Indicates whether Distributed File System (DFS) is enabled. Valid values include: • yes — Allows administrators to group shared folders located on different shares by transparently connecting them to one or more DFS namespaces. • no
BranchCache enabled	Indicates whether BranchCache is enabled. Valid values include: • yes — Copies content from the main office or hosted cloud content servers and caches the content at branch office locations. This allows client computers at branch offices to access content locally rather than over the WAN. • no (default)
Offline availability	Indicates whether Offline availability is enabled. When enabled, users can use this feature on their computers to work with shared folders stored on a server, even when they are not connected to the network. Valid values include: • none — Prevents clients from storing documents and programs in offline cache (default) • documents — All files that clients open will be available offline. • programs — All programs and files that clients open will be available offline. Programs and files will preferably open from offline cache, even when connected to the network. • manual — Only specified files will be available offline.

Create a CIFS snapshot

Create a snapshot CIFS share.

Format
```
/prot/snap/cifs create [-async] -name <value> [-descr <value>]
-snap <value> -path <value> [-enableContinuousAvailability {yes
| no} ] [-enableCIFSEncryption {yes | no } ] [-umask <value> ]
[-enableABE {yes | no} ] [-enableBranchCache {yes | no} ] [-
offlineAvailability {none | documents | programs | manual} ]
```

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.
-name	Type the username of the share.
-descr	Type the description of the share.
-snap	Type the snapshot to associate the share with.
-path	Type the path at which to mount the file system. Default value is /.
-enableContinuousAvailability	Specify whether continuous availability is enabled.
-enableCIFSEncryption	Specify whether CIFS encryption is enabled.
-umask	Type the default Unix umask for new files created on the share.
-enableABE	Specify if Access-based Enumeration is enabled. Valid values include: • yes • no
-enableBranchCache	Specify if BranchCache is enabled. Valid values include: • yes • no
-offlineAvailability	Specify the type of offline availability. Valid values include: • none (default) — Prevents clients from storing documents and programs in offline cache. • documents — Allows all files that clients open to be available offline. • programs — Allows all programs and files that clients open to be available offline. Programs and files will open from offline cache, even when connected to the network. • manual — Allows only specified files to be available offline.

Example

The following command takes a snapshot of a file system with these settings:

• Name is CIFSshare.

• Description is "My share."

• Path is /.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap/cifs
create –name CIFSshare -descr "My share" -path /
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = cifs_1
Operation completed successfully.
```

View snapshot CIFS shares

Lists the existing snapshot CIFS shares.

Format
```
/prot/snap/cifs [{-id <value> | -snap <value>}] show
```

Object qualifier

Qualifier	Description
-id	Identifies the CIFS share.
-snap	Identifies the parent snapshot. The list of shares associated with the identified snapshot will be displayed.

Example
```
uemcli /prot/snap/cifs show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:     ID                 = cifs_2
       Name               = Share_2012-08-24 16:05_00
       Description        =
       Snapshot           = app_1_sg_1
       Local path         = /group.app_1_sg_1.fs.fs_1_wckp
       Export path        = 10.64.76.120:/Share_2012-08-24 16:05_00
       Default access     = na
       No access hosts    =
       Read-only hosts    = 1014[10.192.168.5,10.192.168.6],
1015[10.192.168.9]
       Read/write hosts   = 1016[10.244.245.0/255.255.255.0]
       Root hosts         =
       Creation time      = 2012-08-24 12:18:22
       Last modified time = 2012-08-24 12:18:22
```

Set snapshot CIFS share

Modifies an existing snapshot NFS share.

Format
```
/prot/snap/cifs -id <value> set [-async] [-descr <value>] [-
enableContinuousAvailability {yes | no} ] [-
enableCIFSEncryption {yes | no} ] [-umask <value> ] [-enableABE
{yes | no} ] [-enableBranchCache {yes | no}] [-
offlineAvailability {none | documents | programs | manual} ]
```

Object qualifier

Qualifier	Description
-id	Identifies the snapshot NFS share.

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.
-desc	Specifies the new user description of the share.
-enableContinuousAvailability	Specify whether continuous availability is enabled.
-enableCIFSEncryption	Specify whether CIFS encryption is enabled.
-umask	Type the default Unix umask for new files created on the share.
-enableABE	Specify if Access-Based Enumeration (ABE) is enabled. Valid values include: • yes • no
-enableBranchCache	Specify if BranchCache is enabled. Valid values include: • yes • no
-offlineAvailability	Specify the type of offline availability. Valid values include: • none (default) — Prevents clients from storing documents and programs in offline cache. • documents — Allows all files that clients open to be available offline. • programs — Allows all programs and files that clients open to be available offline. Programs and files will open from offline cache, even when connected to the network. • manual — Allows only specified files to be available offline.

Example

uemcli /stor/prov/sf/cifs -id CIFS_1 set -descr "My share"

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = CIFS_1
Operation completed successfully.
```

Delete snapshot CIFS shares

Delete (destroy) a snapshot CIFS share.

Note

Once you delete a snapshot, you can no longer recover data from it or restore a storage resource to it.

Format
```
/prot/snap/cifs –id <value> delete [-async]
```

Object qualifier

Qualifier	Description
–id	Type the ID of the snapshot to promote.

Action qualifier

Qualifier	Description
–async	Run the operation in asynchronous mode.

Example
The following command deletes snapshot cif_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap/cifs –id cifs_1 delete

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage remote storage systems

Configure remote storage systems that connect to the system to which you are logged in. The system uses the configuration to access and communicate with the remote system. For example, to use remote replication, create a configuration that specifies the remote system to use as the destination for the replication session.

Each remote system configuration is identified by an ID.

The following table lists the attributes for remote storage systems:

Table 85 Remote system attributes

Attribute	Description
ID	ID of the remote system.
Name	Name of the remote system.

Table 85 Remote system attributes (continued)

Attribute	Description
Type	Type of remote system. Value is VNXe or Celerra.
Model	Remote system's model number.
Serial Number	Serial number of the remote system.
Address	Network name or management IP address of the remote system.

Health state	Health state of the storage resource. The health state code appears in parentheses. Value is one of the following:
	
	• OK (5) — Resource is operating normally.
	
	• Degraded/Warning (10) — Working, but one or more of the following may have occurred:
	
	  ▪ One or more of its storage pools are degraded.
	  ▪ Its replication session is degraded.
	  ▪ Its replication session has faulted.
	  ▪ It has almost reached full capacity. Increase the primary storage size, or create additional resources to store your data, to avoid data loss. Change LUN groups on page 251 explains how to increase the primary storage size.
	
	• Minor failure (15) — One or both of the following may have occurred:
	
	  ▪ One or more of its storage pools have failed.
	  ▪ The associated iSCSI node has failed.
	
	• Major (20) — One or both of the following may have occurred:
	
	  ▪ Resource is unavailable.
	  ▪ One or more of the associated storage pools have failed.
	
	• Critical failure (25) — One or more of the following may have occurred:
	
	  ▪ One or more of its storage pools are unavailable.
	  ▪ Resource is unavailable.
	  ▪ Resource has reached full capacity. Increase the primary storage size, or create additional resources to store your data, to avoid data loss. Change LUN groups on page 251 explains how to increase the primary storage size.
	
	• Non-recoverable error (30) — One or both of the following may have occurred:
	
	  ▪ Resource is unavailable.
	  ▪ One or more of the associated storage pools are unavailable.

Health details	Additional health information.
Source user name	For storage systems that are the source in a replication session, the username that is used to access the system.

Remote system attributes (continued)

Attribute	Description
Source user password	For storage systems that are the source in a replication session, the user password that is used to access the system.
Source interfaces	The list of source interface identifiers used to create the interconnect between the two systems.
Destination user name	For storage systems that are the destination in a replication session, the username that is used to access the system.
Destination user password	For storage systems that are the destination in a replication session, the user password that is used to access the system.
Passphrase	The passphrase that is used between the source and destination systems in the replication connection.

Create remote system configurations

Configures a remote system configuration for the local system to access.

Format
```
/remote/sys create -addr <value> -type { VNXe -srcUsername
<value> { -srcPassword <value> | -srcPasswordSecure } -
dstUsername <value> { -dstPassword <value> | -
dstPasswordSecure } | [-sync { enable | disable }] | -name
<value> { -passPhrase <value> | -passPhraseSecure } } [ -srcIf
<value> ] [ -connectionType <value>]
```

Action qualifiers

Qualifier	Description
-addr	Type the network name or IP address of the remote system.
-type	Specifies the remote system type. Value is VNXe.
-srcUsername	For systems that are the source in a replication session, type the username that is used to access the system.
-srcPassword	For systems that are the source in a replication session, type the user password that is used to access the system.
-srcPasswordSecure	Specify the password in secure mode. Once you run the command with this qualifier, you will be asked to type the password separately.
-dstUsername	For systems that are the destination in a replication session, type the username that is used to access the system.
-dstPassword	For systems that are the destination in a replication session, type the user password that is used to access the system.
-dstPasswordSecure	Specify the password in secure mode. Once you run the command with this qualifier, you will be asked to type the password separately.

Qualifier	Description
-name	Specify the remote system name. This qualifier applies to VNX or Celerra systems only.
-passPhrase	Type the passphrase that is used between the source and destination systems in the replication connection. This qualifier applies to VNX or Celerra systems only.
-passPhraseSecure	Specify the password in secure mode. Once you run the command with this qualifier, you will be asked to type the password separately.
-sync	Specify this qualifier to configure a synchronous connection between the source and destination systems.
-connectionType	Specify this qualifier to indicate the type of replication connection. Valid values are async, sync, or both.

Example

The following command creates a remote system configuration with these settings:

- Type is VNXe.

- Network address is 10.64.75.10.

- Includes access credentials for when the system is the source or destination.

The configure remote system receives the ID RS_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/sys create –addr 10.64.75.10 –type vnxe –srcUsername admin1 -srcPassword Password456! –dstUsername admin2 –dstPassword Password986! -connectionType sync

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = RS_1
Operation completed successfully.
```

Verify settings for remote storage systems

Verify the configuration settings for a remote system to ensure that the source storage resource can connect to the remote storage resource.

Format
/remote/sys –id <*value*> verify

Object qualifier

Qualifier	Description
-id	Type the ID of a remote system configuration to verify the settings.

Example

The following command verifies remote system configuration RS_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/sys -id RS_1
verify
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

View settings for remote storage systems

View the configuration for a remote system on the local system. You can filter on the configuration ID of the remote system.

Note

The show action command on page 17 explains how to change the output format.

Format
`/remote/sys [-id <value>] show`

Object qualifier

Qualifier	Description
-id	Type the ID of a remote system configuration.

Example
The following command lists all configurations for remote storage systems:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/sys show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:     ID             = RS_1
       Name           = MyTargetSystem
       Address        = 10.64.74.1
       Type           = VNXe
       Model          = VNXe3200
       Serial number  = FCNCH01234567A90
```

Change settings for remote storage systems

Changes the configuration settings for a remote system.

Format
`/remote/sys -id <value> set [ -name <value> ] [ -addr <value> ] [ -dstUsername <value> { -dstPassword <value> | -dstPasswordSecure } ] [ { -passPhrase <value> | -passPhraseSecure } ] [ -srcIf <value> ]`

Object qualifier

Qualifier	Description
-id	Type the ID of the remote system configuration to change.

Action qualifier

Qualifier	Description
-name	For Celerra systems, type the name of the system.
-addr	Type the network name or management IP address of the remote system.
-dstUsername	For VNXe systems that are the destination in a replication session, type the username that is used to access the system.
-dstPassword	For VNXe systems that are the destination in a replication session, type the user password that is used to access the system.
-dstPasswordSecure	Specify the password in secure mode - the user will be prompted to input the password.
-passPhrase	Type the passphrase that is used between the source and destination systems in the replication connection.
-passPhraseSecure	Specify the password in secure mode - the user will be prompted to input the password.
-srcIf	Specifies the comma separated list of source interfaces to create the interconnect with the remote system. Only one interface per SP may be specified. If the interface is specified for one SP only, the system will automatically select the interface for the second SP.
	Note
	This qualifier is used for VNXe to VNX/Celerra connections only.
	Run the `sys verify` command if the source interface changes.

Example

The following command changes the name, IP address, and access credentials for remote system configuration RS_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/sys -id RS_1
set -name "Remote2" -addr "10.64.74.2" -dstUsername Local/joe -
dstPassword Password456!
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = RS_1

Operation completed successfully.
```

Delete remote system configurations

Deletes the configuration for a remote system.

Note

Before deleting a remote system configuration, ensure that all I/O operations on the system, such as active replication sessions, have completed to avoid data loss.

Format
/remote/sys –id *<value>* delete

Object qualifier

Qualifier	Description
-id	Type the ID of the remote system configuration to delete.

Example
The following command deletes remote system configuration RS_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/sys –id RS_1 delete

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage replication sessions

Storage replication is a process in which storage data is duplicated either locally or to a remote network device. Replication produces a read-only, point-in-time copy of source storage data and periodically updates the copy, keeping it consistent with the source data. Storage replication provides an enhanced level of redundancy in case the main storage backup system fails. As a result:

- Downtime associated cost of a system failure is minimized.
- Recovery process from a natural or human-caused disaster is facilitated.

Each replication session is identified by an ID. The Unisphere online help provides more details about storage replication.

Note

At any given point in time, only one command is supported on a replication session. Before running a new command, ensure that you wait for the existing action on the replication session to complete.

The following table lists the attributes for replication sessions:

Table 86 Replication session attributes

Attribute	Description
ID	ID of the session.
Name	Name of the replication session.
Remote session ID	Identified session in case of replication with the system.

Table 86 Replication session attributes (continued)

Attribute	Description
Synchronization	Type of synchronization. Valid values are: • `auto` — Data is replicated automatically in order to maintain the desired Recovery Point Objective (RPO). • `manual` — Data will only be replicated when manually initiated. **Note** As the RPO increases, the potential for data loss also increases, as well as the amount of required protection space. Lowering the RPO will reduce the amount of potential data loss, but will also increase network traffic and may negatively impact performance. The default RPO is one hour.
RPO	Recovery Point Objective (RPO) interval for automatic synchronization.
Session type	Storage type of the session. Valid value is **block,** which indicates a replication session of a block-based storage resource.
Resource type	Type of storage resource to which the replication session is applied.
State	State of the replication session. Valid values are: • `In Sync` • `Syncing` • `Consistent` • `Out of Sync`
Health state	Health state of the session. Valid values are: • `OK` — Session is operating normally. • `Degraded/Warning` — Session is currently paused. • `Minor failure` — An error has caused one or more of the following: ■ Session has stopped. You can try to resume a stopped replication session. ■ Session has failed over, likely due to the source storage resource becoming unavailable. The destination storage resource is now in a read/write state. Review the state of the source and

Table 86 Replication session attributes (continued)

Attribute	Description
	check your network connections for any problems. Once the source is back online, you can fail back the session to return it to normal operation. ■ Communication with the replication host has been lost. It is likely that the system is either powered down or there is a network connectivity issue between the systems. A change in the network configuration on either side could also interrupt communication. **Note** If the replication session is in an error state, the session will not be recoverable. You will need to delete the session and create a new replication session.
Health details	Additional health information.
Operational status	Operational status of the session. The operational status code appears in parentheses.
Network status	Status of the network connection. Valid values are: ● Unknown — Network status is currently unknown. If you continue to see this value, check the network connections. ● OK — Network connection is operating normally. ● Lost Communication — Communication with the replication host has been lost. It is likely that the system is either powered down or there is a network connectivity issue between the systems. A change in the network configuration on either side could also interrupt communication.
Source status	Status of the source storage resource in the session. Valid values are: ● Unknown — Source status is unknown. ● OK - Source is operating normally. ● Paused — Replication session for the source is currently paused. ● Fatal replication issue — Source has experienced a critical error and the

Table 86 Replication session attributes (continued)

Attribute	Description
	replication session has stopped. Delete the replication session and re-create it.
	• Lost communication — Communication with the replication host has been lost. It is likely that the system is either powered down or there is a network connectivity issue between the systems. A change in the network configuration on either side could also interrupt communication.
	• Failed over — The replication session has failed over to the destination site. In a failover state, the destination object is read/write. When communication is reestablished between the source and destination, the source becomes read-only. To resume operations on the source site, the replication session needs to be failed back.
Destination status	Status of the destination storage resource in the session. Valid values are: • Unknown — Status of the destination resource is unknown. • OK — Destination resource is operating normally. • Paused — Replication session for destination resource is currently paused. • Fatal replication issue — Destination has experienced a critical error and the replication session has stopped. Delete the replication session and re-create it. • Lost communication — Communication with the replication host has been lost. It is likely that the system is either powered down or there is a network connectivity issue between the systems. A change in the network configuration on either side could also interrupt communication. • Failed over — The replication session has failed over to the destination site. In a failover state, the destination object is read/write. When communication is reestablished between the source and destination, the source becomes read-only.

Table 86 Replication session attributes (continued)

Attribute	Description
	To resume operations on the source site, the replication session needs to be failed back.
`Local role`	The local system role. Valid values are: • `Unknown` — Status of the local system is unknown. • `Source` — Resource on the local system is replicated to the remote system. • `Destination` — Resource on the local system is the replication destination of the resource on the remote system. • `Loopback` — Resources participating in the replication session are located on the same storage system. • `Local` — Resources participating in the replication session are located on the different storage processors of the local system.
`Source resource`	ID of the storage resource that is the source of the session. The source can be local or remote.
`Destination type`	Type of destination used in the session. Valid values are: • `local` — Maintain a full copy of the storage resource on the local system. This has advantages over snapshots in that a full copy, not just a copy of changes, is retained. • `remote` — Maintain a full copy of the storage resource on a remote system by transferring the data over the network. Remote replication is often used to ensure that a copy is available at a remote site in case of catastrophic data loss, for example, due to natural disaster at the local site.
`Destination system`	For remote sessions, the ID of the remote system on which the data is replicated.
`Destination resource`	ID of the storage resource on which the data is replicated.
`Time of last sync`	Date and time of the last replication synchronization.
`Sync status`	Percentage of the replication synchronization that has completed and the amount of time remaining.

Table 86 Replication session attributes (continued)

Attribute	Description
`Sync transfer size remaining`	Status of synchronization (percentage and time remaining). For multi-LUN applications there is a comma-separated list of values.
`Sync transfer rate`	Data transfer rate during a replication synchronization. For multi-LUN applications there is a comma-separated list of values.
`Source SP A interface`	ID of the interface on the SPA of the source system for the replication.
`Source SP B interface`	ID of the interface on the SPB of the source system for the replication.
`Destination SP A interface`	ID of the interface on the SPA of the destination system for the replication.
`Destination SP B interface`	ID of the interface on the SPB of the destination system for the replication.
`Previous transfer rate`	Previous transfer rate for the replication session.
`Average transfer rate`	Average transfer rate for the replication session.
`Element pairs in the session`	For LUN group and VMware VMFS datastore replications, the LUN element pairs within the replication.

Create replication sessions

Create a replication session.

Prerequisites
Before creating a replication session, complete the following configuration tasks:

- Create the storage resource that provides the replication source.

- For local replication, create a replication destination on a local system.

- For remote replication, create a replication connection to a remote system, and create a replication destination on that remote system.

Format
```
/prot/rep/session create -srcRes <value> [-srcSPAInterface
<value>] [-srcSPBInterface <value>] -dstType {local|remote –
dstSys <value>} -dstRes <value> [-dstSPAInterface <value>] [-
dstSPBInterface <value>] [-name <value>] [-syncType {manual [-
autoInitiate {yes|no}]|[auto -rpo <value>]]
```

Action qualifiers

Qualifier	Description
`-srcRes`	Type the ID of the storage resource to use as the source.

Qualifier	Description
-srcSPAInterface	Type the ID of the interface on the SPA of the source system for the replication. **Note** This qualifier is used for replications on remote systems only. If the qualifier is not specified, the system identifies the interface automatically.
-srcSPBInterface	Type the ID of the interface on the SPB of the source system for the replication. **Note** This qualifier is used for replications on remote systems only. If the qualifier is not specified, the system identifies the interface automatically.
-dstType	Specify the type of destination. Value is one of the following: local - Maintain a full copy of the storage resource on the local system. This has advantages over snapshots in that a full copy, not just a copy of changes, is retained. remote - Maintain a full copy of the storage resource on a remote system by transferring the data over the network. Remote replication is often used to ensure that a copy is available at a remote site in case of catastrophic data loss, for example, due to natural disaster at the local site.
-dstSys	For remote replication, type the ID of the destination system. View settings for remote storage systems on page 302 explains how to view the IDs of the remote system configuration on the local system.
-dstRes	Type the ID of the destination storage resource. **Note** To get the proper ID in the case of remote replication, you should use a command that list resources on a local machine with the -remSys qualifier. For example: • `uemcli /stor/prov/sf/res -remSys <value> show` • `uemcli /stor/prov/iscsi/res -remSys <value> show` • `uemcli /stor/prov/vmware/nfs -remSys <value> show`
-dstSPAInterface	Type the ID of the interface on the SPA of the destination system for the replication.

Qualifier	Description
	Note This qualifier is used for replications on remote systems only. If the qualifier is not specified, the system identifies the interface automatically.
-dstSPBInterface	Type the ID of the interface on the SPB of the destination system for the replication. **Note** This qualifier is used for replications on remote systems only. If the qualifier is not specified, the system identifies the interface automatically.
-syncType	Specify how the source and destination will synchronize. Valid values are: • `auto` — Data is replicated automatically in order to maintain the desired Recovery Point Objective (RPO). • `manual` — Data will only be replicated when manually initiated. **Note** As the RPO increases, the potential for data loss also increases, as well as the amount of required protection space. Lowering the RPO will reduce the amount of potential data loss, but will also increase network traffic and may negatively impact performance. The default RPO is one hour.
-autoInitiate	Specify whether the system will perform the first replication synchronization automatically. Value is yes or no.
-rpo	Type the time interval for when the synchronization will run. Use the following format: `<HH>[:MM]` Where: • `HH` — Type the number of hours. Range is 00-24 hours (1 day). • `MM` — Type the number of minutes, in 5 minute increments. Range is 05 to 55.

Example

The following command creates a replication session with these settings:

- Source storage resource is file system RS_1.
- Destination system type is remote.
- Remote destination system is RS_2.

- Remote storage resource is file system LUN_2.
- Synchronization type is automatic.
- RPO is 2 hours and 30 minutes.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session create -name REP1 -srcRes RS_1 –dstType remote -dstSys RS_2 –dstRes LUN_2 –syncType auto –rpo 02h30m

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = 81604378625_FCNCH097274B3A_0000_81604378627_FCNCH097274B37_0000
Operation completed successfully.
```

View replication sessions

View details about replication sessions. You can filter on the session ID.

The show action command explains how to change the output format.

Format
```
/prot/rep/session [{-id <value>| -name <value>| -res <value>}]
show
```

Object qualifier

Qualifier	Description
-id	Type the ID of the replication session.
-name	Type the name of the replication session.
-res	Type the ID of a local storage resource on the system to view the sessions associated with it.

Example
The following command displays all replication sessions on the system:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:    ID                 =
42949672967_FNM00134400082_0000_42949672967_FNM00131800278_0000
      Name               = REP1
      Session type       = lun
      Synchronization type = manual
      RPO                = N/A
      Sync State         = syncing
      Health state       = OK (5)
      Operational status = Active (0x840d)
      Time of last sync  = N/A
      Sync status        =
      Element pairs      = N/A
```

Change replication session settings

Change the settings for a replication session.

Format
```
/prot/rep/session {-id <value> | -name <value>} set [-paused
{yes|no [ -forceFullCopy ]}] [ -newName <value> ] [ -
srcSPAInterface <value> ] [ -dstSPAInterface <value> ] [ -
srcSPBInterface <value> ] [ -dstSPBInterface <value> ] [ -
syncType { manual | auto -rpo <value>}]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the replication session to change.
-name	Type the name of the replication session to change.

Action qualifiers

Qualifier	Description
-paused	For automatic synchronization, specify to pause the session. Valid values are: • yes • no
-srcSPAInterface	Type the ID of the interface on the SPA of the source system for the replication. **Note** This qualifier is used for replications on remote systems only. If the qualifier is not specified, the system identifies the interface automatically.
-srcSPBInterface	Type the ID of the interface on the SPB of the source system for the replication. **Note** This qualifier is used for replications on remote systems only. If the qualifier is not specified, the system identifies the interface automatically.
-dstSPAInterface	Type the ID of the interface on the SPA of the destination system for the replication. **Note** This qualifier is used for replications on remote systems only. If the qualifier is not specified, the system identifies the interface automatically.

Qualifier	Description
-dstSPBInterface	Type the ID of the interface on the SPB of the destination system for the replication.
	Note
	This qualifier is used for replications on remote systems only. If the qualifier is not specified, the system identifies the interface automatically.
-syncType	Specify how the source and destination will synchronize. Valid values are:
	• auto — Data is replicated automatically in order to maintain the desired Recovery Point Objective (RPO).
	• manual — Data will only be replicated when manually initiated.
	Note
	As the RPO increases, the potential for data loss also increases, as well as the amount of required protection space. Lowering the RPO will reduce the amount of potential data loss, but will also increase network traffic and may negatively impact performance. The default RPO is one hour.
-rpo	For automatic synchronization, type the time interval for when the synchronization will run. Use the following format:
	<HH>[:MM]
	Where:
	• HH — Type the number of hours. Range is 00-24 hours (1 day).
	• MM — Type the number of minutes, in 5 minute increments. Range is 05 to 55.

Example
The following command changes the source interface and destination interface for replication session
81604378625_FCNCH097274B3A_0000_81604378627_FCNCH097274B37_0000:

```
uemcli /prot/rep/session -id
81604378625_FCNCH097274B3A_0000_81604378627_FCNCH097274B37_0000 set -
srcSPAInterface if_1 -srcSPBInterface if_2 -dstSPAInterface if_3 -
dstSPBInterface if_4
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
ID = 81604378625_FCNCH097274B3A_0000_81604378627_FCNCH097274B37_0000
Operation completed successfully.
```

Manually synchronize replication sessions

Manually synchronize a replication session.

Format
```
/prot/rep/session{-id <value> | -name <value>} sync
```

Object qualifier

Qualifier	Description
-id	Type the ID of the replication session to synchronize.
-name	Type the name of the replication session to synchronize.

Example
The following command initiates a manual resynchronization of replication session REPS_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session -id REPS_1 sync

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Delete replication sessions

Delete a replication session. The deletion process automatically synchronizes the source storage resource with the destination storage resource, makes both read/write, and then deletes the session. You can then connect a host to either storage resource.

Note

Once you delete a replication session, data from the source storage resource will no longer be replicated on the destination, leaving the data unprotected.

Format
```
/prot/rep/session {-id <value> | -name <value>} delete
```

Object qualifier

Qualifier	Description
-id	Type the ID of the replication session to delete.
-name	Type the name of the replication session to delete.

Example
The following command deletes replication session 81604378625_FCNCH097274B3A_0000_81604378627_FCNCH097274B37_0000:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session -id 81604378625_FCNCH097274B3A_0000_81604378627_FCNCH097274B37_0000 delete

```
Storage system address: 10.0.0.1
Storage system port: 443
```

```
HTTPS connection

Operation completed successfully.
```

Fail over replication sessions

Run this command on the destination system to perform a failover of a replication session, with possible data loss, in response to an emergency scenario in which the source becomes unavailable.

After the failover, the destination system is read/write. To reestablish communication between the source and destination, fail back the session that has failed over. Fail back replication sessions on page 317 explains how to fail back a replication session that has failed over.

Note

Failover operations terminate the transfer of data if there is a transfer in progress, causing a potential loss of data. If the source site is still available when you perform a failover, the system attempts to change the source storage resource from read/write to read-only.

Initiate a planned downtime
To initiate a planned downtime, run this command on the source system by specifying the -*sync* option with the value *yes*. When you fail over a replication session from the source system, the destination system is fully synchronized with the source to ensure that there is no data loss. The destination storage resource can be used for providing access to the host.

Format
```
/prot/rep/session { -id <value> | -name <value> } failover [-
sync {yes | no}]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the replication session to fail over.
-name	Type the name of the replication session to fail over.

Action qualifier

Qualifier	Description
-sync	Specifies whether a synchronization needs to be performed before failing over the replication session. Valid values are: • yes • no --- **Note** You cannot use the value yes when initiating a failover from the destination system. ---

Example

The following command performs a fail over of replication session
81604378625_FCNCH097274B3A_0000_81604378627_FCNCH097274B37_0000:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session –
id 81604378625_FCNCH097274B3A_0000_81604378627_FCNCH097274B37_0000
failover
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Fail back replication sessions

Fail back a replication session that has failed over. A failback results in the following:

- Synchronizes the destination and source storage resources.

- Makes the destination storage resource read-only.

- Makes the source storage resource read/write.

When the failback operation is complete, the replication session will resume and you
may connect your hosts to the source storage resource.

Note

Ensure that hosts do not write to the destination storage resource, which will become
read-only.

Format
```
/prot/rep/session {-id <value> | -name <value>} failback [-
forceFullCopy]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the replication session to fail back.
-name	Type the name of the replication session to fail back.

Action qualifier

Qualifier	Description
-forceFullCopy	Specifies to force a full synchronization before the failback operation occurs. **Note** You may lose the common base on the source storage resource as a result of the event that caused the original failover. If there is no longer a common base for the source storage resource, a full synchronization is required. For such cases, ensure that you specify this qualifier.

Example

The following command performs a fail back of replication session
81604378625_FCNCH097274B3A_0000_81604378627_FCNCH097274B37_0000:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session -
id 81604378625_FCNCH097274B3A_0000_81604378627_FCNCH097274B37_0000
failback
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage virtual RecoverPoint appliance CHAP accounts

When configuring a virtural RecoverPoint appliance (RPA) to work with the storage
system, you can optionally set up iSCSI interface authentication using the Challenge
Handshake Authentication Protocol (CHAP). Two type of CHAP are supported:

- Incoming Forward CHAP – This is used by the storage system to authenticate the RPA.
  This CHAP is similar to the iSCSI CHAP account. For more information on configuring
  this CHAP, see Manage iSCSI CHAP accounts for one-way CHAP authentication on
  page 154.

- Outgoing Forward CHAP - This is used by the RPA to authenticate the storage system.

This section describes the attributes and commands that enable you to manage RPA
CHAP accounts.

The following table lists the attributes for RPA CHAP accounts:

Table 87 RPA CHAP attributes

Attribute	Description
Out username	The outgoing CHAP user name.
Out secret	The outgoing CHAP secret (password).
Out secret format	The outgoing CHAP secret input format. Valid values are (case insensitive): • ascii — Secret in the ASCII format (default). • hex — Secret in hexadecimal format.

View the RPA CHAP account

View the RPA CHAP account.

Format
```
/remote/rpa/chap show
```

Example
```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/rpa/chap
show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
```

```
HTTPS connection

1:     Out username  = admin
```

Change RPA CHAP account

Modify the RPA CHAP account.

Format
```
/remote/rpa/chap set [ -outUsername <value>] [ { -outSecret
<value> | -outSecretSecure } [-outSecretFormat {ascii|hex}]]
```

Action qualifier

Qualifier	Description
-outUsername	Type the outgoing CHAP user name.
-outSecret	Type the outgoing CHAP secret (password). By default, the CHAP secret is an ASCII string that is 12 to 16 characters. Hexadecimal secrets are 12 to 16 pairs of data (24 to 32 characters).
-outSecretSecure	Type the outgoing CHAP secret in secure mode. You will be prompted separately to type the password.
-outSecretFormat	The outgoing CHAP secret input format. Valid values are (case insensitive): • ascii - Secret in the ASCII format (default). • hex - Secret in hexadecimal format.

Example
**uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/rpa/chap set
-outUsername admin -outSecret abcdef123456**

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage Common Anti Virus Agent (CAVA)

The following table lists the attributes for CAVA:

Table 88 CAVA attributes

Attribute	Description
NAS server	Associated NAS server identifier.
Enabled	Indicates if CAVA is enabled. Valid values are: • Yes • No

Table 88 CAVA attributes (continued)

Attribute	Description
	Note Values are case-insensitive.

View CAVA settings

View details about CAVA settings.

Format
```
/net/nas/cava [-server <value>] show
```

Object qualifier

Qualifier	Description
-server	Identifies the associated NAS server.

Example
The following command displays the CAVA settings:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/cava show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection


1:     NAS server  = nas_0
       Enabled     = yes

2:     NAS server  = nas_1
       Enabled     = no
```

Change CAVA settings

Modify the CAVA settings.

Format
```
/net/nas/cava -server <value> set -enabled {yes | no}
```

Object qualifier

Qualifier	Description
-server	Identifies the associated NAS server.

Action qualifier

Qualifier	Description
-enabled	Specify whether CAVA is enabled. Valid values are: • yes

Qualifier	Description
	• `no` **Note** Values are case-insensitive.

Example

The following command enables CAVA:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/cava -server nas_1 set -enabled yes

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

CHAPTER 8

Manage Events and Alerts

This chapter addresses the following topics:

View event logs and alerts

The system monitors and reports on a variety of system events. It collects the events and writes them to the user log. The log contains a record for each event. Some log entries generate alerts. Alerts are usually events that require attention from the system administrator and typically indicate a system problem. For example, you might receive an alert telling you that a disk has faulted, or that the system is low on storage capacity.

In Unisphere, events appear as messages and alerts. Unisphere CLI displays additional event attributes that provide more detailed event reports than what appear in Unisphere. Configure alert settings on page 327 explains the commands for configuring alerts. The Unisphere online help provides more details on logs and alerts.

Each event record and alert is identified by an ID.

The following table lists the attributes for event records:

Table 89 Event record attributes

Attribute	Description
Message ID	ID of the event record.
Description	Brief description of the event.
Severity	Severity of the event. Valid values are: • `critical` – An error has occurred that has a significant impact on the system and should be remedied immediately. • `error` – An error has occurred that has a minor impact on the system and should be remedied at some point but does not need to be fixed immediately. • `warning` – An error has occurred that you should be aware of but has not had a significant impact on the system. • `notice` – An important event has occurred that does not have an impact on the functioning of the system. • `info` – Some event has occurred that does not have an impact on the functioning of the system. **Note** Values are case-insensitive.
Time	Date and time when the event occurred, in Greenwich Mean Time (GMT).
Node	Name of the SP that generated the event. Value is SPA or SPB.
Process	ID of the system process that generated the event.
Category	Event category. **Note** After a successful login to the system, when you run a command through the CLI, events that include the category attribute with the Authentication value will appear twice as there are separate events for successful login and authentication.

Table 89 Event record attributes (continued)

Attribute	Description
Account	User account of the user that caused the event. N/A appears if a user did not cause the event or the account is unavailable.
Component	System component that caused the event. Intended for service personnel.
Product	System product that caused the event. Intended for service personnel.

View event records

View a detailed log of system events. Each event is a record in the log and each record is identified by an ID. You can display 100 event records at a time and filter on a range of times when the events were logged and the event severity.

Note

explains how to change the output format.

Format
```
/event/log show [-fromTime <value>] [-toTime <value>] [-limit
<value>] [-severity {critical | error | warning | notice |
info}]
```

Action qualifiers

Qualifier	Description
-fromTime	Type the beginning of the time interval for which to display event records. The format is YYYY-MM-DD HH:MM:SS. **Note** If you omit this qualifier, the list of logs that appears will begin with the first log.
-toTime	Type the end of the time interval for which to display event records. The format is YYYY-MM-DD HH:MM:SS. **Note** If you omit this qualifier, the value is the current system time.
-limit	Type the maximum number of records to display. The value cannot exceed the default number 100.
-severity	Type the minimum severity level of the events to display. For example, if you type **critical,** records for the alert and emergency severities will also appear.

Example
The following command lists all event logs generated on 11/09/2009 up to 23:59:59 GMT:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/log show -
fromTime "2009-11-09 00:00:00.000" -to "2009-11-09 23:59:59.999"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      Message ID  = Login success
        Description = User admin authenticated in authority
LocalDirectory/Local
        Severity    = info
        Time        = 2009-11-09 19:43:08.577
        Node        = spa
        Account     = unix/spa/root
        Component   = Server
```

View alert history

View a detailed list of all system alerts. The alert history clears each time the system reboots.

The following table lists the attributes for alerts:

Table 90 Alert attributes

Attribute	Description
Time	Date and time (in GMT) when the alert occurred.
Message	Alert message.
Description	Description of a problem.
Severity	Alert severity. Valid values are: • `critical` – An error has occurred that has a significant impact on the system and should be remedied immediately. • `error` – An error has occurred that has a minor impact on the system and should be remedied at some point but does not need to be fixed immediately. • `warning` – An error has occurred that you should be aware of but has not had a significant impact on the system. • `notice` – An important event has occurred that does not have an impact on the functioning of the system. • `info` – Some event has occurred that does not have an impact on the functioning of the system. **Note** Values are case-insensitive.

Note

The show action command on page 17 explains how to change the output format.

Format
```
/event/alert/hist show
```

Example

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/hist show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection


1:      Time        = 2009-11-09 19:43:08.577
        Message     = Message text
        Description = Description text
        Severity    = info

2:      Time        = 2009-11-09 19:55:18.321
        Message     = Message text
        Description = Description text
        Severity    = info
```

Configure alert settings

Specify how the system handles alerts, which are notifications of system and user events. You can have the alerts sent directly to your service provider and e-mailed to specific addresses. You can also have the system send alerts as traps to an SNMP destination. Configure SNMP destinations for alerts on page 330 provides more details on setting up a destination to receive alerts over SNMP. View event logs and alerts on page 324 provides details about viewing the current logs and alerts.

Note

To send e-mail alerts, you must configure an SMTP server on the system as explained in Manage SMTP server settings on page 125.

The following table lists the attributes for alerts:

Table 91 Alert attributes

Attribute	Description
Enable ConnectEMC (if supported)	Indication of whether ConnectEMC is enabled. Valid values are: • yes • no ConnectEMC sends e-mail alerts to EMC service to help with resolving customer problems. This setting requires an SMTP server explained in Manage SMTP server settings on page 125.
Include contact information	Indicates whether customer contact information is included in dial home events. Valid values are (case insensitive): • yes • no
ConnectEMC mode (if supported)	Defines which server to use for ConnectEMC - ESRS or SMTP. Valid values are: • esrs • smtp

Table 91 Alert attributes (continued)

Attribute	Description
Language	Language in which the system sends e-mail alerts.
E-mail from address	E-mail address the system uses as the FROM address.
E-mail to addresses	Comma-separated list of e-mail addresses to send alerts.
E-mail severity threshold	Minimal severity of alerts the system will send as e-mail. Valid values are: • `critical` — An error has occurred that has a significant impact on the system and should be remedied immediately. • `error` — An error has occurred that has a minor impact on the system and should be remedied at some point but does not have to be fixed immediately. • `warning` — An error has occurred that you should be aware of but has not had a significant impact on the system. • `notice` — An important event has occurred that does not have an impact on the functioning of the system. • `info` — Some event has occurred that does not have an impact on the functioning of the system. **Note** Values are case-insensitive.
SNMP severity threshold	Minimal severity of alerts the system will send as SNMP traps. Valid values are: • `critical` — An error has occurred that has a significant impact on the system and should be remedied immediately. • `error` — An error has occurred that has a minor impact on the system and should be remedied at some point but does not have to be fixed immediately. • `warning` — An error has occurred that you should be aware of but has not had a significant impact on the system. • `notice` — An important event has occurred that does not have an impact on the functioning of the system. • `info` — Some event has occurred that does not have an impact on the functioning of the system. **Note** Values are case-insensitive.
SNMP version	Version of SNMP that the destination is running.
SNMP engine ID	SNMP engine ID for the SNMP destination.

View alert settings

View the settings for how the system handles alerts.

Note

The show action command on page 17 explains how to change the output format.

Format

```
/event/alert/conf show
```

Example

**uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/conf
show**

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      Enable ConnectEMC           = no
        Include contact information = yes
        Language                    = english
        E-mail from address         = me@mail.com
        E-mail to addresses         = joe@mail.com,rick@mail.com
        E-mail severity threshold   = Info
        SNMP severity threshold     = Info
        SNMP version                = 3.0
        SNMP engine ID              =
```

Configure alert settings

Configure the settings for how the system handles alerts.

Note

For e-mail alerts to work, you must configure an SMTP server on the system, as explained in Manage SMTP server settings on page 125.

Format

```
/event/alert/conf set [-enableConnectEMC {yes|no}] [-
includeContactInfo {yes | no}] [-emailFromAddr <value>] [-
emailToAddrs <value>] [-emailSeverity {critical|error|warning|
notice |info}] [-snmpSeverity {critical|error|warning|notice|
info}]
```

Action qualifiers

Qualifier	Description
-enableConnectEMC (if supported)	Enable the system to send e-mail alerts to EMC service. Valid values are (case insensitive): • yes • no
-includeContactInfo	Specify whether customer contact information is included in dial home events. Valid values are (case insensitive): • yes

Qualifier	Description
	• `no`
`-emailFromAddr`	Type the e-mail address the system will use as the FROM address. The addresses will appear in the FROM field of the recipient's e-mail application.
`-emailToAddrs`	Type a comma-separated list of e-mail addresses the system will send alerts.
`-emailSeverity`	Specify the minimal severity of alerts the system will send as e-mails. Values are: • `critical` • `error` • `warning` • `notice` • `info`
`-snmpSeverity`	Specify the minimal severity of alerts the system will send as SNMP traps. Values are: • `critical` • `error` • `warning` • `notice` • `info`

Example

The following command changes these alert settings:

- Connect EMC is enabled.

- FROM address is admin@mail.com.

- TO addresses are jason@mail.com and pete@mail.com.

- Minimum alert severity for sending e-mail alerts is info.

- Minimum alert severity for sending alerts as SNMP traps is error.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/conf
set -enableConnectEMC yes -includeContactInfo no -emailFromAddr
me@mail.com -emailToAddrs "jason@mail.com,pete@mail.com" -
emailSeverity info -snmpSeverity error
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Configure SNMP destinations for alerts

The system uses the Simple Network Management Protocol (SNMP) to transfer system alerts as traps to an SNMP destination host. Traps are asynchronous messages that

notify the SNMP destination when system and user events occur. The three types of traps are:

- Information – Provide routine status information about system operation.
- Warnings – Indicate that a problem has occurred or may occur.
- Errors – Report system problems that occurred or are occurring.

You can configure the types of alert information the system reports (informational, error, or emergency indications).

Each SNMP destination is identified by an ID.

The following table lists the attributes for SNMP destinations:

Table 92 SNMP destination attributes

Attribute	Description
ID	ID of the SNMP destination.
Host	Hostname or IP address of the SNMP destination.
Port	Host port on the SNMP destination that will receive the traps.
User name	Username that is used to access the SNMP destination.
Auth protocol	Protocol that is used to authenticate access to the SNMP destination. Value is one of the following: • none — No authentication • md5 — Message-Digest algorithm 5 • sha — Secure Hash Algorithm
Auth password	Authentication password for accessing the SNMP destination.
Privacy protocol	Protocol that is used to enable privacy on the SNMP destination. The privacy protocol encrypts the SNMP packets. Value is one of the following: • none — No encryption • aes — Advanced Encryption Standard • des — Data Encryption Standard
Privacy password	Privacy password for the privacy protocol.

Create SNMP destination

Create an SNMP trap destination for system alerts.

Format

```
/event/alert/snmp create -host <value> -port <value> -userName
<value> [ -authProto { none | md5 { -authPassword <value> | -
authPasswordSecure } [ -privProto { none | aes { -privPassword
<value> | -privPasswordSecure } | des { -privPassword <value> |
-privPasswordSecure } } ] | sha { -authPassword <value> | -
authPasswordSecure } [ -privProto { none | aes { -privPassword
<value> | -privPasswordSecure } | des { -privPassword <value> |
-privPasswordSecure } } ] } ]
```

Action qualifiers

Qualifier	Description
–host	Type a hostname or IP address of the SNMP destination.
-port	Type the host port on the SNMP destination that will receive the traps.
–userName	Type the username that is used to access the SNMP destination.
-authProto	Specify the protocol that is used to authenticate access to the SNMP destination. Value is one of the following: • none — No authentication • md5 — Message-Digest algorithm 5 • sha — Secure Hash Algorithm
-authPassword	Type the authentication password.
-authPasswordSecure	Specify the password in secure mode - the user will be prompted to input the password.
-privProto	Specify the protocol that is used to enable privacy on the SNMP destination. Value is one of the following: • none — No encryption • aes — Advanced Encryption Standard • des — Data Encryption Standard
-privPassword	Type the privacy password.
-privPasswordSecure	Specify the password in secure mode - the user will be prompted to input the password.

Example

The following command creates an SNMP destination with these settings:

• Host IP is 10.64.75.1.

• Host port is 333.

• Username is user1.

• Authorization protocol is md5.

• Authorization password is authpassword1234.

• Privacy protocol is des.

• Privacy password is privpassword321.

The SNMP destination receives ID Host1_333:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/snmp create –host 10.64.75.1 –port 333 –userName user1 authProto md5 – authPassword authpassword1234 –privProto des –privPassword privpassword321

```
Storage system address: 10.0.0.1
Storage system port: 443
```

```
HTTPS connection

ID = Host1_333
Operation completed successfully.
```

View SNMP destinations

View details about SNMP destinations. You can filter on the SNMP destination ID.

Note

explains how to change the output format.

Format
```
/event/alert/snmp [-id <value>] show
```

Object qualifier

Qualifier	Description
-id	Type the ID of an SNMP destination.

Example
The following command lists all SNMP destinations:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/snmp show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID               = Host1_323
        Host             = Host1
        Port             = 323
        User name        = user1
        Auth protocol    = md5
        Privacy protocol = aes
```

Change SNMP destination settings

Change the settings for an SNMP destination.

Format
```
/event/alert/snmp -id <value> set [ -host <value> ] [ -port
<value> ] [ -userName <value> ] [ -authProto { none | md5 { -
authPassword <value> | -authPasswordSecure } [ -privProto
{ none | aes { -privPassword <value> | -privPasswordSecure } |
des { -privPassword <value> | -privPasswordSecure } } ] | sha
{ -authPassword <value> | -authPasswordSecure } [ -privProto
{ none | aes { -privPassword <value> | -privPasswordSecure } |
des { -privPassword <value> | -privPasswordSecure } } ] } ]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the SNMP destination to change.

Action qualifiers

Qualifier	Description
-host	Type a hostname or IP address of the SNMP destination.
-port	Type the host port on the SNMP destination that will receive the traps.
-userName	Type the username that is used to access the SNMP destination.
-authProto	Specify the protocol that is used to authenticate access to the SNMP destination. Value is one of the following: • none — No authentication • md5 — Message-Digest algorithm 5 • sha — Secure Hash Algorithm
-authPassword	Type the authentication password.
-authPasswordSecure	Specify the password in secure mode - the user will be prompted to input the password.
-privProto	Specify the protocol that is used to enable privacy on the SNMP destination. Value is one of the following: • none — No encryption • aes — Advanced Encryption Standard • des — Data Encryption Standard
-privPassword	Type the privacy password.
-privPasswordSecure	Specify the password in secure mode - the user will be prompted to input the password.

Example

The following command changes the authorization protocol, privacy protocol, authorization password, and privacy password for SNMP destination Host1_323:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/snmp –id Host1_323 set -authProto md5 -authPassword newauthpassword –privProto des –privPassword newprivpassword

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = Host1_323
Operation completed successfully.
```

Delete SNMP destinations

Delete an SNMP destination.

Note

If you delete an SNMP destination, the system will stop sending alerts to it as traps.

Format

```
/event/alert/snmp -id <value> delete
```

Object qualifier

Qualifier	Description
-id	Type the ID of an SNMP destination to delete.

Example

The following command deletes SNMP destination Host1_323:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/snmp -id Host1_323 delete

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

CHAPTER 9

Service the System

This chapter addresses the following topics:

Change the service password

The system ships with a default Service password for performing service actions on the system. After you change the password, the old Service password will not work.

Prerequisites
Both Storage Processors (SPs) must be present in the system and their boot mode must be Normal Mode. If you have removed an SP or an SP has failed, you must replace the SP before you can change the Service password.

Format
```
/service/user set { -passwd <value> | -passwdSecure } { { -
oldpasswd <value> | -oldpasswdSecure } | -force }
```

Action qualifiers

Qualifier	Description
-passwd	Type a new Service password. The following are the password requirements: • Passwords must be 8 to 40 characters in length and cannot contain spaces. • Passwords must include mixed case, a number, and a special character from this list: ! , @ # $ % ^ * ? _ ~ • When changing a password, do not reuse any of the last 3 passwords.
-passwdSecure	Specify the password in secure mode - the user will be prompted to input the password and the password confirmation.
-oldpasswd	Type the old password to set the new password.
-oldpasswdSecure	Specify the password in secure mode - the user will be prompted to input the password.
-force	Specify whether it is a password modification request or a password reset request. This is intended to be used by service user only.

Example
The following command changes the Service password. Note that this can only be executed in normal mode.:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /service/user set -passwd NewPassword456! -oldpasswd OldPassword456!

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Service actions

Apply service action to the system. This command must be executed with service user credentials.

Restart management software

Restarts management software on the system. Can be executed in normal mode only.

Format
```
/service/system restart
```

Example
The following command restarts system management software:

uemcli /service/system restart

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Shut down the system

Shuts down the system.

Note

This command can be executed in normal mode only.

Format
```
/service/system shutdown
```

Example
The following command shuts down the system (in normal mode only):

uemcli /service/system shutdown

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Reinitialize the system

Reinitialize the storage system. System should be in the service mode to execute this action.

Format
```
/service/system reinit
```

Example
The following command reinitializes the storage system:

```
uemcli /service/system reinit
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Collect service information

Collect information about the system and save it to a file. The file may then the be downloaded by the uemcli -download command. (See View the switches on page 346).

Format
```
/service/system collect {-serviceInfo | -config [-
showPrivateData] }
```

Action qualifiers

Qualifier	Description
-serviceInfo	Collect information about the system and save it to a .tar file. Service providers can use the collected information to analyze the system.
-config	Create a snapshot of the current system configuration and save it to a file. It captures all of the data necessary to recreate the current configuration on a new or reinitialized system. It does not capture log files or other types of diagnostic data.
-showPrivateData	Include sensitive information (such as IP addresses) into the collected data.

Example
The following command collects information about the system and saves it to a file:

```
uemcli /service/system collect -serviceInfo
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully
```

SSH access

Manage SSH (Secure shell) access to the system. This command must be executed with service user credentials.

Set SSH access

Manage SSH access to the system.

Format
```
/service/ssh set -enabled {yes | no}
```

Action qualifiers

Qualifier	Description
-enabled	Flag indicating whether the SSH access is enabled. The following are the password requirements. Value is one of the following: • Yes • No

Example

The following command enables SSH access to the system:

uemcli /service/ssh set -enabled yes

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

View SSH settings

Displays SSH settings.

Format
```
/service/ssh show
```

Example

The following command displays SSH settings:

uemcli /service/ssh show

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:    SSH enabled   = yes
```

Service the storage processor (SP)

Allows user to apply service action to the storage processor. This command must be executed with service user credentials.

Enter service mode

Switch the storage processor to the service mode.This command can only be executed in normal mode.

Format
```
/service/sp -id <value> service
```

Object qualifier

Qualifier	Description
-id	Identifies the storage processor.

Example

The following command enters the service mode:

```
uemcli /service/sp -id spa service
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Reboot

Reboot the storage processor.

Format

```
/service/sp -id <value> reboot
```

Object qualifier

Qualifier	Description
-id	Identifies the storage processor.

Example

```
uemcli /service/sp -id spa reboot
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Reimage

Reimage the storage processor.

Format

```
/service/sp -id <value> reimage
```

Object qualifier

Qualifier	Description
-id	Identifies the storage processor.

Example

```
uemcli /service/sp -id spa reimage
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Service the cache card

Allows user to apply service action to the cache card. Service user credentials are required to execute this command.

Reboot the cache card

Reboot the cache card.

Format
```
/service/ccard -id <value> reboot
```

Object qualifier

Qualifier	Description
-id	Identifies the storage processor.

Example

uemcli /service/ccard -id Ccard_0 reboot

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

CHAPTER 10

Use Switches

This chapter addresses the following topics:

View the switches

The Unisphere CLI switches apply only to your installed Unisphere CLI client. Use the switches to access a system, upload files to the system, and manage security certificates.

Format
`uemcli [{-help|-h|-?}]`
The following table describes each of the switches:

Table 93 Switches

Switch	Description
-destination|-d	IP (IPv4 or IPv6) address or network name of the destination system. If you do not include this switch, the client uses the addresses specified for -default. If no default address exists, the client uses the localhost address 127.0.0.1.
-port	Port number on the system.
-user|-u	Username for logging in to the system.
-password|-p	Password for logging in to the system.
-securePassword	Specifies the password in secure mode - the user will be prompted to input the password.
-timeout|-t	Timeout (in seconds) after which you are automatically logged out of the system due to user inactivity or a system problem. The default value is 600 seconds (10 minutes).
-sslPolicy	Policy for handling unknown SSL certificates downloaded from the system. Value is one of the following: • `interactive` — Prompt the user to accept the certificates for the current session (default). • `reject` — Automatically reject the certificates. • `accept` — Automatically accept the certificates. • `store` — Automatically accept and store the certificates.
-certList	List of all certificates stored locally in the lockbox.
-certClear	Delete all certificates stored locally in the lockbox.
-certDel	Delete one or more certificates from the lockbox. Type a comma-separated list of certificate IDs. **Note** Use `-certlist` to view a list of stored certificates with their IDs.
-certImport	Import a certificate from a file. Supported formats are: • Privacy Enhanced Mail (PEM) • Distinguished Encoding Rules (DER) • Cryptographic Message Syntax (PKCS #7)

Table 93 Switches (continued)

Switch	Description
-syntax|-s	Syntax name and version (optional) to use in the client. Separate the name and version with a colon. For example, the following switch applies the UEM version 1.5 syntax: `-syntax uem:1.5`

-upload	Upload a file to the system. Type the file type and location in the following format:
	
	`{-help|<type> -help|{-f|-file} <file> <type>`
	`[<parameter>=<value>...]}`
	
	where:
	
	• `-help` — Display a list of file types you can upload to the system.
	
	• `type -help` — Display information about a file type. Value is one of the following:
	
	  ■ `license` — A license file. During upload the license is installed on the system.
	
	  ■ `upgrade` — A system software upgrade candidate file. When you upload an upgrade candidate file onto your system, it replaces the previous version. There can be only one upgrade candidate on the system at a time. Upgrade the system software on page 53 explains upgrading the system software using an uploaded upgrade candidate.
	
	  ■ `/net/nas/ldap` — A custom LDAP schema or a Certification Authority (CA) certificate for the NAS server identified by a mandatory `-server` parameter. Uploading a valid LDAP schema changes the LDAP configuration. This will result in changes to the file systems access on the specific NAS server. For more information, see Upload an LDAP schema on page 83.
	
	  ■ `/net/nas/server` — A custom user mapping rules file for the specific NAS server identified by a mandatory `-id` parameter.
	
	• `-f|-file file type` — For `file`, type the path and filename of the file to upload. For `type`, type the file type to upload.
	
	• `parameter = value` — Optional parameter=value pairs for including specific parameters during the upload.
	
	Note
	For a list of supported file types, type `-upload -help`

-download	Download a file from the system. Type the file type and location in the following format:
	
	`{-help | <type> -help | {-d <folder> | -f <file>} <type> [-`
	`<parameter> <value> ...]}`
	
	where:
	
	• `-help` — Display a list of file types you can download from the system.

Table 93 Switches (continued)

Switch	Description
	• `type -help` — Display information about a file type. Value is one of the following: ■ `serviceInfo` — Save service information about your system to a .tar file. Your service provider can use the collected information to analyze your system. This action should be executed with service user credentials. To download service information you should collect it at first using the `uemcli /service/system collect -serviceInfo` command. **Note** Contact your service provider determine if it is necessary to collect this information and to establish a process for sending the file to customer support. **Note** ■ `config` — Save details about the configuration settings on the storage system to a file. Service personnel can use this file to assist you with reconfiguring your system after a major system failure or a system reinitialization. This action should be executed with service user credentials. The file only contains details about your system configuration. You cannot restore your system from this file. This action should be executed with service user credentials. **Note** It is recommended that you save the file to a remote location after every major system configuration change, to ensure that you always have a current copy of the file available. ■ `/net/nas/ldap` — A custom LDAP schema for the NAS server identified by a mandatory `-server` parameter. Once you configure LDAP settings for a NAS server, you can download the automatically generated LDAP schema file to make additional changes. For more information, see Download an LDAP schema on page 84. ■ `/net/nas/server` — A custom user mapping rules file for the specific NAS server identified by a mandatory `-id` parameter. • `{-d <folder> | -f <file>} <type>` — Destination directory or path to the destination file. For ‹type›, enter the type of file to download. • `[-<parameter> <value>...] [<action>]` — Download a file from the storage system. • `<type>` — File type. • `[-<parameter> <value> ...]` — Optional key-value pairs that are passed to the storage system via URL encoded parameters separated by spaces.

Table 93 Switches (continued)

Switch	Description
	• `[<action>]` — Optional action indicating what shall be executed on the file downloaded.
`-download`	Enter the location of the target file to download from the storage system and the location where you want to store the file. Use the following format: `-download <target> <localpath>` where: • `<target>` — Path to the file to download. • `<localpath>` — Path to the location to store the file.
`-gmtoff`	Greenwich Mean Time (GMT) offset for converting the time on the system to the time on the client system. Type **auto** to send the offset of the current client system. Type the following to specify the offset: `[-|+]<HH>[:<MM>]` where: • `-|+` — Type the sign of the GMT offset. If the offset is ahead of GMT, you can omit the plus sign. • `HH` — Type the hours for the offset. • `MM` — Type the minutes for the offset (optional). Separate the minutes from the hours with a colon.
`-help|-h|-?`	Display information about the syntax and switches.
`-saveUser`	Save the access credentials specified for the `-user` and `-password` switches to a local security file in the lockbox. With the access credentials saved, Unisphere CLI automatically applies them to the specified system destination and port pair each time you run a command. Save Unisphere CLI settings on page 354 explains saving user account credentials to the local client system.
`-removeUser`	Remove the specified user account from the lockbox.
`-default`	Save the destination and port pair as the default system to access. When you run a command, Unisphere CLI will run the command on the default system. Unisphere CLI saves the specified destination and port pair to a local security file in the lockbox. Each time you include the `-default` switch, Unisphere CLI overwrites the previous saved destination and port pair with the current destination and port pair. If you include the `-port` switch, the specified port value is paired with the `-destination` value and saved to the local security file. Save Unisphere CLI settings on page 354 explains saving user account credentials to the local client system.
`-silent`	Allow a command to complete by suppressing the output and not requiring user confirmation. This is useful when there are commands in scripts.

Table 93 Switches (continued)

Switch	Description
`-noHeader`	Hide the header message (system IP address, port number, and so on) that appears above the command output. Hide header information on page 352 explains how to hide the header from the output.
`-v`|`-version`	Display the version of your Unisphere CLI.
`-cmdTime`	Display the current time on the destination system.

Access the system

To access and run commands on a system through Unisphere CLI, specify the network name or management IP address of the system, your username, and your password.

Note

Unisphere CLI does not provide a session mode in which you log in to the system once and run commands. You must type the destination system, your username, and your password each time you run a command. Doing so logs in to the system, runs the command, and then logs out. To avoid having to type the access credentials each time you run a command, include the `-saveUser` switch to save the username and password for the specified destination system and port pair.

Format
```
[{-d|-destination} <value>] [{-u|-user} <user_name>] [{-p|-
password} <password>]
```

Switches

Qualifier	Description
`-destination`|`-d`	IP address or network name of the destination system. If you do not include this switch, the client uses the addresses specified for `-default`. If no default address exists, the client uses the localhost address 127.0.0.1.
`-user`|`-u`	Domain and username for logging in to the system. For example, Local/joe.
`-password`|`-p`	Password for logging in to the system.
`-securePassword`	Specifies the password in secure mode - the user will be prompted to input the password.
`-port`	Specify the port number through which to access the system. **Note** If you do not include the `-port` switch, Unisphere CLI accesses the system through default port 443.
`-default`	Save the destination and port pair as the default system to access. When you run a command, Unisphere CLI runs the command on the default system. Unisphere CLI saves the

Qualifier	Description
	specified system and port pair to a local file. Each time you include the `-default` switch, Unisphere CLI overwrites the previously saved destination and port pair with the current destination and port pair.
	Note
	If you include the `-port` switch, the specified port value is paired with the **-destination** value and saved to the local file. Hide header information on page 352 explains saving user account credentials on the local client system.
`-saveUser`	Save the access credentials specified for the `-user` and `-password` switches to a local file. With the access credentials saved, Unisphere CLI automatically applies them to the specified destination and port pair each time you run a command. Hide header information on page 352 explains saving user account credentials on the local client system.
`-removeUser`	Remove saved access credentials for the specified destination and port pair.

Example 1

The following example accesses the destination system 10.0.0.1 as user Local/joe with password 12345:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456!
```

Example 2

The following example saves the access credentials for the specified user:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! -saveUser
```

Example 3

The following example sets the destination system as the default:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! -default
```

Example 4

The following example accesses the default system:

```
uemcli -u Local/joe -p MyPassword456!
```

Example 5

The following example removes the saved access credentials from destination system 10.0.0.1:

```
uemcli -d 10.0.0.1 -removeUser
```

Upload and upgrade candidate

To upgrade the system software, upload an upgrade candidate file that you download from the support website and use the `-upload` qualifier. Once you upload the candidate file to the system, use an upgrade session to start the upgrade process. Create upgrade sessions on page 53 explains configuring upgrade sessions.

Prerequisites

Download the latest system software upgrade candidate from the support website.

Format

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! -upload -f
<file> upgrade
```

Options

Qualifier	Description
-f	Type the path and file name of the upgrade candidate file to upload. Wrap the path and file name in quotes.

Example

The following example upload a upgrade candidate file to the system:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! -upload -f "

\upgrade_image\upgrade-2.0.0.12190-MAGNUM-RETAIL.tgz.bin" upgrade

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Hide header information

Each time you run a switch or command, the header message appears. The header displays the destination system, system port number, the syntax, and communication protocol used (HTTPS). For example:

```
Storage system address: 127.0.0.1
Storage system port: 443
HTTPS connection
```

To hide the header, include the -noHeader switch:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! -noHeader /sys/

general show

```
1:     System name           = Vorpal
       Model                 = EMC Storage Systems 12GB RAM WM PHTM
       Platform type         = EMC Storage System
       Product serial number = FNM00102000154
       Auto failback         = on
       Health state          = Degraded/Warning (10)
```

Manage SSL certificates

When logging in to the system through Unisphere CLI, the system uses Secure Socket Layer (SSL) certificates to secure communications between the CLI client and the system. You can manage these certificates and configure a policy for the Unisphere CLI to use when receiving unknown certificates. All downloaded certificates are stored in the secure, local lockbox on the client system. Save Unisphere CLI settings on page 354 explains how settings are saved.

Configure a certificate policy

Set up a certificate policy to specify how Unisphere CLI will automatically respond to unknown SSL certificates downloaded from the system.

Format
```
-sslPolicy <value>
```

Switch

Switch	Description
-sslPolicy	Value is one of the following: • `interactive` — Client prompts the user to take action (default). • `reject` — Client automatically rejects the certificates. • `accept` — Client automatically accepts the certificates. • `store` — Client automatically accepts and stores the certificates in the lockbox.

View certificates

View a list of all SSL certificates stored in the lockbox.

Note

The show action command on page 17 explains how to change the output format.

Format
```
-certList
```

Delete certificates

Delete one or more SSL certificates from the lockbox.

Format
```
-certDel <certificate IDs>
```

Switch

Switch	Description
-certDel	Type a comma-separated list of certificate IDs to delete. **Note** Use `-certList` to view a list of stored certificates with their IDs.

Clear all certificates

Delete all SSL certificates from the lockbox.

Format
```
-certClear
```

Import certificates

Import a SSL certificate from a file.

Format
`-certImport <file>`

Switch

Switch	Description
`-certImport`	Type the path and name for the file to import. Supported formats are: • Privacy Enhanced Mail (PEM) • Distinguished Encoding Rules (DER) • Cryptographic Message Syntax (PKCS #7)

Save Unisphere CLI settings

You can save the following settings on the host on which you run Unisphere CLI:

• User access credentials, including your username and password, for each system you access. For more information, see the -saveUser switch in View the switches on page 346.

• SSL certificates imported from the system. For more information on SSL certificates, see Manage SSL certificates on page 352.

• Information about default system to access through Unisphere CLI, including the system name or IP address and the system port number. For more information, see the -default switch in View the switches on page 346.

Unisphere CLI saves the settings to a secure lockbox that resides locally on the host on which Unisphere CLI is installed. The stored data is only available on the host where it was saved and to the user who saved it. The lockbox resides in the following locations:

• On Windows XP:

```
C:\Documents and Settings\<account_name>\Local Settings
\Application Data\EMC\UEM CLI\
```

• On Windows 7:

```
C:\Users\${user_name}\AppData\Local\.EMC\UEMCLI
```

• On UNIX/Linux:

```
<home_directory>/EMC/UEM CLI
```

The cps.clb and csp.clb.FCD files are lockbox-related. If you uninstall Unisphere CLI, these directories and files are not deleted, giving you the option of retaining them. However, for security reasons, you may want to delete these files.

CHAPTER 11

Manage Metrics

This chapter addresses the following topics:

Manage metrics service

Storage system metrics gather information about system performance and storage usage, and collect that information for user review. Analyzing the system metrics can help predict the future growth of the system.

Historical and real-time metrics values are available in predefined intervals. High frequency (short interval) metric values are not kept as long as low frequency (long interval) metrics.

The following table lists the metrics service attributes:

Table 94 Metrics service attributes

Attribute	Description
History enabled	Indicates whether historical metrics collection is enabled. Value is one of the following: • Yes • No Default value is yes.
History retention	Identifies the timestamp of the earliest available value for each frequency interval. The formats are: • YYYY-MM-DD HH:MM:SS (5 sec) • YYYY-MM-DD HH:MM:SS (60 sec) • YYYY-MM-DD HH:MM:SS (300 sec) • YYYY-MM-DD HH:MM:SS (3600 sec) • YYYY-MM-DD HH:MM:SS (14400 sec) If the data for a certain interval is not available, the system displays not available instead of a timestamp. **Note** By default, the timestamps are UTC time. If you specify a timezone offset with -gmtoff, the timestamps adjust accordingly.

View metrics service settings

View the current metrics service settings.

Note

explains how to change the output format.

Format
```
/metrics/service show
```

Example
The following command displays the metrics service settings for the system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/service
show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection


1:  History enabled  = yes
    History retention= 2012-9-20 12:00:00 (5 sec), 2012-9-20 12:00:00
(60 sec), 2012-9-14 12:00:00 (300 sec), not available (3600 sec), not
available (14400 sec)
```

Configure metrics service

Enable historical metrics collection.

Format
```
/metrics/service set -historyEnabled { yes | no }
```

Note

Only administrators are allowed to run this command.

Action qualifiers

Qualifier	Description
-historyEnabled	Indicates whether historical metrics collection is enabled or disabled. Value is one of the following: • Yes • No Default value is Yes. **Note** The system prompts for confirmation if you specify No.

Example
The following command enables metrics collection:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/service set
-historyEnabled
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection


Operation completed successfully.
```

Manage metrics settings

Storage system metrics gather information about system performance and storage usage, and collect that information for user review. Analyzing the system metrics can help predict the future growth of the system.

The following table lists the metrics attributes:

Table 95 Metrics attributes

Attribute	Description
Path	Unique ID for the metric. **Note** Metrics are usually associated with objects. This association is reflected by a * character in the metric path, such as **sp.*.net.device.*.bytes**, which is associated with two objects, SP and network device. The metrics commands will accept a metric path with the * replaced by an object, and return only the result for the specified object. The system generates an error if the specified object is not valid.
Description	Description of the metric.
Type	Metric type. Valid values are: • rate — A counter difference relative to a unit of time. • counter — A monotonically increasing, unsigned quantity. • fact — Represents point-in-time information. Fact values should be expected to go up and down. • 64 bits counter — A counter of 64 bits. • text — Literal.
Unit	Unit measure for the metric.
Availability	Availability of the metric. Value is one of the following: • Historical — The metric is included in historical metrics collection. • Real-time — The metric supports real-time subscription. • Historical, real-time — The metric supports both historical and real-time collection. This attribute does not apply to family, set, and compound metrics.

View metrics settings

View information about supported metrics.

Note

explains how to change the output format.

Format
```
/metrics/metric [-path <value>] [-availability { historical |
real-time } ] show
```

Object qualifier

Qualifier	Description
-path	Specify a comma-separated list of metric paths.

Qualifier	Description
	Note When typing metric paths, replace . with \., , with \, and \ with \\ in the object names. Omitting this switch specifies all available metrics.
`-availability`	Specify a type of metric to display. Value is one of the following: • `Historical` • `Real-time` Omitting this switch displays all metrics.

Example

The following command displays the metrics service settings for the system:

**uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/metric -
path
sp.*.storage.lun.*.avgReadSize,sp.*.storage.filesystem.*.writesRate,sp
.*.cifs.smb2.basic.readsRate show -detail**

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:  Path         = sp.*.storage.lun.*.avgReadSize
    Description  = Average read size on this LUN
    Type         = fact
    Unit         = KB
    Availability = historical, real-time

2:  Path         = sp.*.storage.filesystem.*.writesRate
    Description  = Rate of sp.*.storage.filesystem.*.writes
    Type         = rate
    Unit         = Requests/s
    Availability = historical, real-time

3:  Path         = sp.*.cifs.smb2.basic.readsRate
    Description  = Rate of sp.*.cifs.smb2.basic.reads
    Type         = rate
    Unit         = Ops/s
    Availability = real-time
```

Manage historical metrics values

Storage system metrics gather information about system performance and storage usage, and collect that information for user review. Analyzing the system metrics can help predict the future growth of the system.

Historical metric values are available in predefined intervals. High frequency (short interval) metric values are not kept as long as low frequency (long interval) metrics.

The following table lists the historical metrics attributes:

Table 96 Historical metrics attributes

Attribute	Description
`Timestamp`	Time when the metric value was collected. The format is: `YYYY-MM-DD HH:MM:SS`, where: • `YYYY` — Year • `MM` — Month • `DD` — Day • `HH` — Hour • `MM` — Minute • `SS` — Second
`Dynamic attributes`	Identifies the object name or metric value.

View historical metrics settings

View historical metrics settings. The output appears in a tabular format.

Note

explains how to change the output format.

Format

```
/metrics/value/hist -path <value> show -interval { 5 | 60 | 300
| 3600 | 14400 }[ -from <value> ] [ -to <value>] [ -count
<value> ][ -flat ][ -summary ]
```

Object qualifier

Qualifier	Description
`-path`	Specify a comma-separated list of metric paths. **Note** When typing metric paths, replace . with \., , with \, and \ with \\ in the object names.
`-interval`	Specify an interval for the metric values. Default interval is seconds.
`-from`	Specify the start of the query period. The format is: `YYYY-MM-DD HH:MM:SS` or `YYYY-MM-DDTHH:MM:SS`, where: • `YYYY` — Year • `MM` — Month • `DD` — Day • `T` — Time delimiter • `HH` — Hour • `MM` — Minute

Qualifier	Description
	• `SS` — Second
	Note
	Ensure that the value is a time in the past. You can choose to specify just the date (in the `YYYY-MM-DD` format) or the time (in the `HH:MM:SS` format). If you do not specify the time, the system automatically uses 00:00:00. If you choose to not specify the date, the current system date is used.
`-to`	Specify the end of the query period. The format is: `YYYY-MM-DD HH:MM:SS` or `YYYY-MM-DDTHH:MM:SS`, where: • `YYYY` — Year • `MM` — Month • `DD` — Day • `T` — Time delimiter • `HH` — Hour • `MM` — Minute • `SS` — Second
	Note
	Ensure that the value is a time in the past. You can choose to specify just the date (in the `YYYY-MM-DD` format) or the time (in the `HH:MM:SS` format). If you do not specify the time, the system automatically uses 00:00:00. If you choose to not specify the date, the current system date is used.
`-count`	Specify the number of samples to display. A sample is a set of metric values related to a single timestamp. Valid values are numbers greater than or equal to one.
`-flat`	Displays the member values for grouped metrics.
`-summary`	Displays the maximum, minimum, and average value for each metric.

Note

The `-from` and `-to` qualifiers take precedence over the `-count` qualifier. In the example below, only 7 samples exist between the from and to dates. Although the value for the `-count` qualifier is set to 10, only 7 values appear. If the `-from` and `-to` qualifiers are not specified, the output will include 10 samples.

Example

The following command displays historical metrics for the system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/value/hist
-path sp.*.fs.filesystem.*.file.*.readBytes show -from "2012-07-08
12:17:30" -to "2012-07-08 12:19:30" -count 10 -interval 60
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Timestamp           | SP   | File System | File   | Read Bytes
--------------------+------+-------------+--------+-----------
2012-07-08 12:17:30 |  spa|          fs1|     f11|       4000
                    |  spa|          fs1|     f12|       5000
                    |  spa|          fs2|     f21|       6000
                    |  spb|          fs1|     f11|       7000
                    |  spb|          fs1|     f12|       8000
                    |  spb|          fs2|     f21|       9000
                    |  spb|          fs2|     f23|       9000
```

Examples of output with different combinations of the `-from`**,** `-to`**, and** `-count`
qualifiers

The following table illustrates the output that appears with combinations of the `-from`, `-to`, and `-count` qualifiers. It assumes that the current time is 2012-09-21 12:30:00.

Qualifier Combination	Output
`-from <future date/ time>`	**Example:** `-from` "2012-09-21 12:31:00" **Result:** This results in an error because the time for the `-from` qualifier is specified in the future.
`-from <current date/ time or date/time in the past>` `-to <future date/ time>`	**Example:** `-from` "2012-09-01 00:00:00" `-to` "2012-09-21 12:31:00" **Result:** This results in an error because the time for the `-to` qualifier is specified in the future.
`-from <date/time in the past> -count <value>`	**Example:** `-from` "2012-09-20 01:02:00" `-count` 100 **Result:** The result includes 100 samples from "2012-09-20 01:02:00". If there are less than 100 samples available, the result lists all samples from the specified time to the current time.

`-from <date/time in the past>`
 `-to <current date/ time or date/time in the past>`
 `-count <value>`
	Example: `-from` "2012-09-20 01:02:00" `-to` "20-09-20 12:00:00" `-count` 100
	 Result: The result includes 100 samples within the specified time period. If there are less than 100 samples available, the result lists all samples within the time period.

`-to <current date/ time or date/time in the past>` `-count <value>`	**Example:** `-to` "20-09-20 12:00:00" `-count` 100 **Result:** The result includes the latest 100 samples before the specified time. If there are less than 100 samples available, the result lists all samples.
`-count <value>`	**Example:** `-count` 100 **Result:** The result includes the latest 100 samples, or if there are less than 100 samples available, the result lists all samples.

Qualifier Combination	Output
`-to <current date/ time or date/time in the past>`	**Example:** `-to` "20-09-20 12:00:00" **Result:** The result includes all samples from the timestamp of the earliest sample to the specified time.
`-from, -to, and - count are not specified.`	**Result:** The result includes the latest 100 samples, or if there are less than 100 samples available, the result lists all samples. This is equivalent to "`-count 100`".

Manage real-time metrics values

Storage system metrics gather information about system performance and storage usage, and collect that information for user review. Analyzing the system metrics can help predict the future growth of the system.

The following table lists the real-time metrics attributes.

Table 97 Real-time metrics attributes

Attribute	Description
`Timestamp`	Time when the metric value was collected. The format is: `YYYY-MM-DD HH:MM:SS`, where: • `YYYY` — Year • `MM` — Month • `DD` — Day • `HH` — Hour • `MM` — Minute • `SS` — Second
`Dynamic attributes`	Identifies the object name or metric value.

View real-time metrics settings

View real-time metrics settings. The output appears in a tabular format.

Note

explains how to change the output format.

Format
```
/metrics/value/rt -path <value> show -interval <value> [ -to
<value>] [ -count <value> ][ -flat ][ -summary ]
```

Object qualifier

Qualifier	Description
`-path`	Specify a comma-separated list of metric paths.

Qualifier	Description
	Note When typing metric paths, replace . with \., , with \, and \ with \\ in the object names.

Action qualifier

Qualifier	Description
`-interval`	Specify an interval for the metric values. Default interval is seconds.
`-to`	Specify the end of the query period. The format is: `YYYY-MM-DD HH:MM:SS` or `YYYY-MM-DDTHH:MM:SS`, where: • `YYYY` — Year • `MM` — Month • `DD` — Day • `T` — Time delimiter • `HH` — Hour • `MM` — Minute • `SS` — Second **Note** Ensure that the value is a time in the past. You can choose to specify just the date (in the `YYYY-MM-DD` format) or the time (in the `HH:MM:SS` format). If you do not specify the time, the system automatically uses 00:00:00. If you choose to not specify the date, the current system date is used.
`-count`	Specify the number of samples to display. A sample is a set of metric values related to a single timestamp. Valid values are numbers greater than or equal to one.
`-flat`	Displays the member values for grouped metrics.
`-summary`	Displays the maximum, minimum, and average value for each metric.

Example

The following command displays real-time metrics for the system:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! uemcli /metrics/ value/rt -path sp.*.cifs.client.*.readCalls show -interval 10 -output nvp

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:  Timestamp = 2012-07-08 12:17:30
    SP        = spa
```

```
    Client    = c1
    CIFS Read = 100

2:  Timestamp = 2012-07-08 12:17:30
    SP        = spb
    Client    = c1
    CIFS Read = 100


3:  Timestamp = 2012-07-08 12:18:40
    SP        = spa
    Client    = c1
    CIFS Read = 100

4:  Timestamp = 2012-07-08 12:18:40
    SP        = spa
    Client    = c2
    CIFS Read = 100

5:  Timestamp = 2012-07-08 12:18:40
    SP        = spb
    Client    = c1
    CIFS Read = 100

6:  Timestamp = 2012-07-08 12:19:50
    SP        = spa
    Client    = c1
    CIFS Read = 100

7:  Timestamp = 2012-07-08 12:19:50
    SP        = spb
    Client    = c1
    CIFS Read = 100
```

APPENDIX A

Reference

This appendix addresses the following topics:

Storage resource size limitations

The following table lists the size restrictions when creating or resizing a storage resource.

Table 98 Storage resource size limitations

Storage resource type	Minimum size	Default size	Maximum size
File systems	1 GB	100 GB	16 TB
LUN storage	1 Block	100 GB	16 TB
VMware datasores (NFS and VMFS)	1 GB	100 GB	16 TB

Health details

Health details attribute contains a user-friendly description of the health status of the component. When applicable, it also includes a URL to the online help or support page that provides steps to resolve a problem. A component may have multiple description strings indicating the health of the relevant subcomponents. For example:

```
Health details = "The storage resource has failed because it uses a
storage pool that includes one or more disks with problems. Remedy
the problem with the disks. (http://10.0.0.1/alerts/context_sensitive/
dpe_invalid_disk.htm)","An I/O module in your disk-processor
enclosure (DPE) may have faulted. Reboot the storage processor (SP).
If the problem persists after the reboot, replace the I/O module.
(http://10.0.0.1/alerts/context_sensitive/replace_failed_part.htm)"
```