Dell EMC Unity™ Family

Version 4.5

Unisphere® Command Line Interface User Guide

P/N 302-002-578 REV 06

Published January 2019

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS-IS.“ DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

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

CONTENTS

Chapter 3 Configure Network Communication 121

Additional resources

As part of an improvement effort, revisions of the software and hardware are periodically released. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features. Contact your technical support professional if a product does not function properly or does not function as described in this document.

Where to get help
Support, product, and licensing information can be obtained as follows:

Product information
For product and feature documentation or release notes, go to Unity Technical Documentation at: www.emc.com/en-us/documentation/unity-family.htm.

Troubleshooting
For information about products, software updates, licensing, and service, go to Online Support (registration required) at: https://Support.EMC.com. After logging in, locate the appropriate **Support by Product** page.

Technical support
For technical support and service requests, go to Online Support at: https://Support.EMC.com. After logging in, locate **Create a service request**. To open a service request, you must have a valid support agreement. Contact your Sales Representative for details about obtaining a valid support agreement or to answer any questions about your account.

Special notice conventions used in this document

⚠ DANGER

Indicates a hazardous situation which, if not avoided, will result in death or serious injury.

⚠ WARNING

Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

⚠ CAUTION

Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

NOTICE

Addresses practices not related to personal injury.

Note

Presents information that is important, but not hazard-related.

CHAPTER 1

Introduction

This chapter contains the following topics:

Overview

The 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. The Unisphere CLI is intended for advanced users who want to use commands in scripts for automating routine tasks.

Use the 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 SMB 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 NFS, VMFS, and Virtual Volume (VVol) datastores.

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` (default)	The certificate verification process will be used to access the array.

Run the following command:

```
/opt/emc/uemcli/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 28.

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 (-).

View the switches on page 29 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.

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 25 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 21.

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. Action commands on page 22 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 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/configuring, viewing, and deleting. This section explains each of these four action commands. Unisphere CLI syntax on page 20 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. Some options for certain objects cannot be configured when creating the object, but can be configured after the object is creating using the `set` command. This guide often refers to those actions as **configure** actions. 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: • nvp — The name-value pair (NVP) format displays output as name=value. Name-value pair format on page 24 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 24 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 24 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. View the switches on page 29 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]
```

Note

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.
```

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 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 23 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)

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 3 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. Valid values are: • `interactive` (default) — Prompt the user to accept the certificates for the current session. • `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)
`-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>...]}`

Table 3 Switches (continued)

Switch	Description
	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. ■ `/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. ■ `/net/nas/server` — A custom user mapping rules file for the specific NAS server identified by a mandatory `-id` parameter. The mandatory `-type` parameter specifies the corresponding type of uploaded configuration file. Valid values are: – `userMapping` – `passwd` – `group` – `hosts` – `netgroup` – `homedir` ■ `/net/nas/cava` — An antivirus configuration file with parameters of the CAVA service. ■ `/net/nas/kerberos` — A Kerberos Key Table (keytab) file, which is required for secure NFS with a custom UNIX or Linux Kerberos KDC. It contains service principal names (SPNs), encryption methods, and keys for the secure NFS service. ■ `/sys/cert` — A certificate file of a particular type for the specific service identified by mandatory `-type` and `-service` parameters. • `-f|-file file type` — For `file`, type the path and filename of the file to upload. For `type`, type the file type to upload.

Table 3 Switches (continued)

Switch	Description
	• `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. • `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 to determine if it is necessary to collect this information and to establish a process for sending the file to customer support. ▪ `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`

Table 3 Switches (continued)

Switch	Description
	parameter. Once you configure LDAP settings for a NAS server, you can download the automatically generated LDAP schema file to make additional changes. ■ `/net/nas/server` — A custom user mapping rules file for the specific NAS server identified by a mandatory `-id` parameter. The mandatory `-type` parameter specifies the corresponding type of uploaded configuration file. Valid values are: – `userMapping` – `passwd` – `group` – `hosts` – `netgroup` – `homedir` ■ `/net/nas/cava` — A CAVA configuration file. ■ `/net/nas/kerberos` — Kerberos Key Table (keytab) file, which is required for secure NFS with custom UNIX or Linux Kerberos KDC. It contains service principal names (SPNs), encryption methods, and keys for secure NFS service. ■ `/import/session/nas` — A detailed file import status report that may contain error information for a VDM to NAS import session identified by the mandatory `-id` parameter. ■ `/sys/cert` — A certificate file present on the storage system identified by the mandatory `-id` parameter. ■ `encryption` — Three types of data at rest encryption (D@RE) files are available for downloading using the mandatory `-type` parameter. Valid values are: – `backupKeys` - When a copy of the keystore is requested, no additional parameters are required. It is recommended that a copy of the keystore be downloaded and saved whenever the provisioned or hardware configuration on the storage system changes. – `auditLog` - When a copy of the auditlog is requested, the mandatory `-entries` parameter must be supplied, where there are two options: `all` or YYYY-MM. All entries can be requested or a specific year and month of entries. The

Table 3 Switches (continued)

Switch	Description
	downloaded file has a maximum size of 100MB. If all the entries will not fit into this file size, the head of the storage system's auditlog will be returned. The remainder of the auditlog can be retrieved using the year and month option. **Note** When the auditlog is requested, its checksum file will be downloaded with it as well. – `cksum` - Requests a regenerated checksum file for a previously downloaded auditlog file. In this case the mandatory `-logName` *<auditlog filename>* parameter must be supplied. **Note** This must be the exact filename of a previously downloaded auditlog file. ■ `/service/system/dump` — Core dump files are generated after an SP failure. Download these files to send to your service provider to help troubleshoot and resolve system issues. Service account credentials are required. • `{-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. • `[<action>]` — Optional action indicating what shall be executed on the file downloaded.
`-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.

Table 3 Switches (continued)

Switch	Description
`-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. **Note** Only one set of credentials for the system can be saved at a time. This means that if the Service password is different than the admin password, you cannot access the CLI with the service user account with`-saveUser` enabled.
`-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.
`-silent`	Allow a command to complete by suppressing the output and not requiring user confirmation. This is useful when there are commands in scripts.
`-noHeader`	Hide the header message (system IP address, port number, and so on) that appears above the command output.
`-v|-version`	Display the version of your Unisphere CLI.
`-cmdTime`	Display the current time on the destination system.
`-enableStdErr`	Write error messages to stderr instead of stdout.
`-flatten`	Display all object names in a flattened format instead of tree format for help information.

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. The `-saveUser` switch only supports one set of saved credentials for the system. This means that this switch should not be enabled if the admin and service passwords are different, as this will prevent successful log in of the service account into the CLI.

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 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 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

Qualifier	Description
	saved, Unisphere CLI automatically applies them to the specified destination and port pair each time you run a command. Hide header information 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 an 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 52 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-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)
```

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 29.
- SSL certificates imported from the system. For more information on SSL certificates, see Manage SSL certificates on page 28.
- 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 29.

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\uemcli`
- On Windows 7 and Windows 10: `C:\Users\${user_name}\AppData\Local\.emc\uemcli`
- On UNIX/Linux: `<home_directory>/.emc/uemcli`

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 2

Manage the System

This chapter contains 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 4 General system attributes

Attributes	Description
`System name`	Name of the system.
`UUID base`	Base value used to generate UUIDs in the host environment (such as OVMS hosts).
`Model`	System model.
`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`	Indication of whether auto failback is enabled for the SP. Valid values are: • `on` • `off`
`Health state`	Health state of the system. The health state code appears in parentheses. Valid values are: • `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

Table 4 General system attributes (continued)

Attributes	Description
	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.
`Power (Present)` (physical deployments only)	Present system power consumption.
`Power (Rolling Average)` (physical deployments only)	Average system power consumption (in the past hour with 30-second sampling rate)

View system settings

View the current system settings.

Note

The show action command on page 23 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
      UUID Base                = 0
      Model                    = Unity 300
      Platform type            = EMC Storage System
```

```
       System UUID              =
       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
       Supported SP upgrades    = SP400, SP500, SP600
```

Example 2 (virtual deployments only)

The following command displays the general settings for a virtual system:

Note

The `UUID Base` does not display when the `-detail` option is not specified.

```
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                   = UnityVSA
        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>] [-uuidBase <value>] [-
autoFailback {on|off}]
```

Action qualifiers

Qualifier	Description
`-name`	Type a name for the system.
`-uuidBase`	Type the UUID Base value.
`-autoFailback`	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

Manually fail back all failed over NAS servers to their original SP. If auto failback is enabled, failback occurs automatically.

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 = Error: The health check has failed. An internal
error is preventing
the health check from completing successfully. Record the error
code and search the
EMC Online Support website for available support options.
[Error Code: platform::check_boot_control_status_2]

Operation completed successfully.
```

Note

- The results of the health check may show errors and warnings, but a message of `Operation completed successfully.` displays in the output. This is only an indication that the health check action was performed, not that it was successfully completed without errors and warnings. Attempt to resolve all errors and rerun the health check.
- If errors occur, a system software upgrade is not allowed. If warnings occur, they can be bypassed during the upgrade procedure.

Configure system information

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

The following table lists the system information attributes:

Table 5 System information attributes

Attribute	Description
`Location name`	Location name
`Address 1`	Contact address for the system
`City`	City name
`State`	State or province name
`Country`	Two-letter country code
`Postal Code`	Postal code
`Contact first name`	First name of the user.
`Contact last name`	Last name of the user.
`Contact mobile phone`	Mobile phone number of the user.
`Contact company`	Company of the user.
`Site ID`	Internal ID for identifying where the system is installed.
`Contact email address`	Contact email address for the system
`Contact phone number`	Contact phone number for the system

View system information

View current system information.

Note

The show action command on page 23 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:     Contact first name    = Zach
       Contact last name     = Arnold
       Contact company       = EMC
       Contact email address = something@somemail.com
       Contact phone number  = 123456789
```

Change system information

Change the system information attributes.

Format

```
/sys/info set [-location <value>] [-contactFirstName <value>]
[-contactLastName <value>] [-contactEmail <value>] [-
contactPhone <value>] [-contactMobilePhone <value>]
```

Action qualifiers

Qualifier	Description
-location	Specify an updated location name.
-contactEmail	Specify the new contact email address for the system.
-contactPhone	Specify the new contact phone number for the system.
-contactMobilePhone	Specify the new contact mobile phone number for the system.
-contactFirstName	Specify the new contact first name for the system.
-contactLastName	Specify the new contact last name for the system.

Example

The following command changes the following system information:

- Contact first name
- Contact last name
- Contact email
- Contact phone
- System location
- Contact mobile phone

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/info set -
contactFirstName Zach -contactLastName Arnold -contactEmail
something@someemail.com -contactPhone 1233456789 -location here -
contactMobilePhone 987654321
```

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

```
HTTPS connection
Operation completed successfully.
```

Manage software versions

See details about the system software versions that have been uploaded to the system manually by a user, or that have been automatically pushed down to the system by support.

Note

Support will not push down any software images to the system without prior user consent.

Table 6 System software attributes

Attribute	Description
`ID`	ID of the system software.
`Type`	System software type. Value is one of the following: • `installed` — Software image that is currently installed on the system • `candidate` — Upgrade candidate uploaded to the system for upgrading the system software • `downloaded`—Software image that was automatically pushed to the system by support.
`Version`	Software version.
`Release date`	Software release date.
`Reboot required`	Indication of whether a reboot is required for this software upgrade package. Values are: • `yes` • `no`
`Pause allowed`	Indication of whether the software upgrade package allows the user to pause the upgrade and choose the desired disruptive upgrade window. Values are: • `yes` • `no`
`Image filename`	Filename of the software image.

View system software versions

Display details about the version of the installed system software any upgrade candidates that have been uploaded to the system. Upgrade the system on page 51 explains how to upgrade the system software.

Format

```
/sys/soft/ver [{-id <value>|-type {installed|candidate|
downloaded}}] 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. • `downloaded` — Software image that was automatically pushed to the system by support.

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         = 4.3.0.1498853411
      Release date    = 2017-06-30 23:33:44
      Image type      =
      Reboot required =
      Pause allowed   =
      Image filename  =

2:    ID              = CAND_1
      Type            = candidate
      Version         = 4.3.0.1502142551
      Release date    = 2017-08-08 05:19:50
      Image type      = software
      Reboot required = yes
      Pause allowed   = yes
      Image filename  = Unity-c4dev_PIE_471-
upgrade-4.3.0.1502142551-4.3.0.1502142551-GNOSIS_DEBUG.tgz.bin

3:    ID              = ASD_1
      Type            = downloaded
      Version         = 4.2.0.9215195
      Release date    =
      Image type      = software
      Reboot required =
      Pause allowed   =
      Image filename  = Unity-_dev_001-
upgrade-4.2.0.9215195.9215195-4.2.0.9215195.9215195-
GNOSIS_DEBUG.tgz.bin.gpg

4:    ID              = ASD_2
      Type            = downloaded
      Version         = V2-Dec-19-2016
      Release date    =
      Image type      = firmware
      Reboot required =
      Pause allowed   =
      Image filename  = Unity-Drive-Firmware-V2-
Dec-19-2016.tgz.bin.gpg
```

Prepare system software version

Prepare an automatically downloaded software image for installation.

Note

Support will not push down any software images to your system without prior user consent.

Format

```
/sys/soft/ver -id <value> prepare
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the automatically downloaded system software.

Example 1

The following command prepares automatically downloaded software image "ASD_1" for installation:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/soft/ver -id
ASD_1 prepare
```

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

Operation completed successfully.
```

Example 2

The following command shows the error that is returned when trying to prepare an image that was not an automatically downloaded software candidate:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/soft/ver -id
CAND_1 prepare
```

```
Operation failed. Error code: 0x6000cd5
The specified image ID is invalid. The current action can only be
performed on downloaded images. Obtain the image ID with '/sys/soft/
ver -type downloaded show' and try again with correct image ID.
(Error Code:0x6000cd5)
```

Note

Use the /sys/soft/ver show command to obtain the ID of any automatically downloaded software images on the system. The "Type" should be "downloaded" such as in the following example:

```
      ID              = ASD_1
      Type            = downloaded
      Version         = 4.2.0.9215195
      Release date    =
      Image type      = software
      Reboot required =
      Pause allowed   =
      Image filename  = Unity-_dev_001-
upgrade-4.2.0.9215195.9215195-4.2.0.9215195.9215195-
GNOSIS_DEBUG.tgz.bin.gpg
```

View faulted storage resources

This topic is to be used as a template for Unity CLI task topics.

This command shows a list of which storage resources are in faulted states, including their health status details.

Format

/sys/res/health/fault

Example

The following example lists the storage resources that are in a faulted state, the type of resource, and the corresponding health state information.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/res/health/fault show

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

1:     ID                   =    pool_1
       Type                 =     pool
          Health state      =    Degraded/Warning (10)

2:     ID                   =    sv_2
          Type                 =     lun
          Health state      =    Minor failure (15)
```

Upgrade the system

Create an upgrade session to upgrade the system 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.

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. If any system components are degraded, the update will fail. Perform a system health check on page 45 explains how to run a health check on the system.

The following table lists the attributes for upgrade sessions.

Table 7 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. • `paused`— Upgrade session has paused before rebooting the SPs. • `failed`— Upgrade session has failed.
`Progress`	Current progress of the upgrade session.
`Creation time`	Date and time 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.
`Percent complete`	Indicates the progress of the upgrade in percent.
`Type`	The type of upgrade being performed: software upgrade or storage processor upgrade. With software upgrade, details can be found with `/sys/soft/ver show`.
`Additional info`	Additional information about the status of the upgrade.

Create upgrade sessions

Creates a new upgrade session. This could be a software or hardware upgrade that is monitored by a session.

NOTICE

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

Format

```
/sys/upgrade create –type { software [-candId <value>] [-pauseBeforeReboot] | sp -newSPModel <value>} [-offline]} [-pauseBetweenReboots]
```

Action qualifiers

Qualifier	Description
-candId	Type the ID of the uploaded upgrade candidate. View system software versions on page 48 explains how to view the ID of the uploaded software candidate. **Note** This argument is optional. If unspecified, the system looks up the upgrade candidate.
-pauseBeforeReboot	Specify whether to pause during the upgrade, executing all tasks before the SPs reboot. **Note** This option is ignored for language packs, hot fix, and ODFU upgrades.
-newSPModel	Start a storage processor upgrade with the specified target model. The possible values for this system are identified using `/sys/general show`.
-offline	Optional parameter that will start an offline storage processor upgrade rather than an online (default) storage processor upgrade.
-pauseBetweenReboots	Optional parameter for software or online Data-in-place (DIP) upgrades. If specified, the system will pause after the first SP has been upgraded, but before the second SP is upgraded. This will allow you to suspend the upgrade until you manually resume the upgrade using `/sys/upgrade resume`.

Example 1

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

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/upgrade create -type software

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

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.

Example 2

The following command creates a session to upgrade the storage processor:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/upgrade create
-type sp -newSPModel SP500
```

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

Operation completed successfully.
```

Example 3

The following command initiates an offline DIP upgrade.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/upgrade create
-type sp -newSPModel SP500 -offline
```

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

Operation completed successfully.
```

Example 4

The following command initiates a software upgrade that pauses after the first SP reboots.

```
uemcli /sys/upgrade create -type software -pauseBetweenReboots
```

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

Operation completed successfully.
```

View upgrade sessions

View details for an existing upgrade session.

Note

The show action command on page 23 explains how to change the output format.

Format

```
/sys/upgrade show
```

Example 1

The following command displays details about the hardware upgrade session:

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

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

1:     Type                 = SP
       Status               = Running
       Status message      =
       Creation time       = 2015-11-09 19:43:08
       Elapsed time        = 01h 3m 08s
       Estimated time left = 01h 70m 00s
       Progress            = Task 2 of 5 (Running health checks)
       Percent complete    = 5%
```

Example 2

The following command displays details about the software upgrade session:

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

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

1:     Type                = Software
       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%
```

Example 3

The following command shows an issue with the pre-upgrade health check in `Additional info`.

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

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

1:     Type                = Software
       Status              = Failed
       Creation time       = 2009-11-09 18:04:12
       Elapsed time        = 00h 20m 08s
       Estimated time left =
       Progress            =
       Percent complete    = 5%
       Additional info     = "Error: The health check has failed.
An internal error is preventing the health check from completing
successfully. Record the error code and search the EMC Online
Support website for available support options. [Error Code:
platform::check_boot_control_status_2]","Error: One or more LUNs
are in degraded state. Record the error code and contact your
service provider. [Error Code:
flr::check_if_lun_recovery_is_required_2]"
```

Resume upgrade session

Resume an existing upgrade session that has been paused or has failed.

Format

`/sys/upgrade resume`

Example

The following command continues with the upgrade.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/upgrade resume
```

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


Operation completed successfully.
```

Cancel upgrade session

Cancel an upgrade session that is failed or paused. If there is a failure with lock (later steps of OS upgrade or storage processor upgrade), the upgrade cannot be canceled and must be "resume" instead.

Format

```
/sys/upgrade cancel
```

Example

The following command cancels the upgrade session.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/upgrade cancel
```

```
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 8 Security settings attributes

Attributes	Description
`FIPS 140 mode`	Indicates whether the system is working in FIPS mode. Valid values are: • `enabled` • `disabled` **Note** Default value is disabled.
`TLS 1.0 mode`	Indicates whether the system has TLS 1.0 enabled. Valid values are: • `enabled` • `disabled`

Table 8 Security settings attributes (continued)

	Note Default value is enabled.
`Restricted shell mode`	Indicates whether the storage processor has restricted shell enabled for the Service account. Valid values are: • `enabled` • `disabled` **Note** Default value is enabled.

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
   TLS 1.0 mode           = enabled
   Restricted shell mode = enabled
```

Change security settings

Change the system security settings.

Format

```
/sys/security set {-fips140Enabled {yes | no} | -tls1Enabled
{yes | no}} | -restrictedShellEnabled {yes | no}[-
restrictedShellDisabledTimeout <value>]}
```

Action qualifiers

Qualifier	Description
`-fips140Enabled`	Enables or disables FIPS 140 compliance mode. Valid values are: • `yes` • `no`

Qualifier	Description
`-tls1Enabled`	Enables or disables TLS 1.0 protocol. Valid values are: • `yes` • `no`
`-restrictedShellEnabled`	Enables or disables restricted shell on the storage processor for the Service account. Valid values are: • `yes` • `no`

Examples

The following command changes the system security setting for FIPS 140 mode:

`uemcli /sys/security set -fips140Enabled yes`

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
The system will reboot one SP at a time for this change to take
effect. Do you want to continue?
yes / no: yes

Operation completed successfully.
```

The following command changes the system security setting for TLS 1.0 protocol:

`uemcli /sys/security set -tls1Enabled no`

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
Please refer to the security configuration guide for backward
compatibility. You will need to manually reboot both SPs for this
change to take effect. Do you want to continue?
yes / no: yes

Operation completed successfully.
```

The following command changes the system security setting for restricted shell enabled setting:

`uemcli /sys/security set -restrictedShellEnabled no`

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
This action will disable restricted shell for service account on
the storage processor. Do you want to continue?
yes / no: yes

Operation completed successfully.
```

Manage system time

The following table lists the system time attributes:

Table 9 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>

Qualifier	Description
	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. Valid values are: • `noreboot` • `allowreboot` • `allowdu` **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.
- Whether the support contracts list is updated automatically on a weekly basis.
- Whether cloud management is enabled for services like Cloud IQ.

The following table lists the support configuration attributes:

Table 10 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.
`Cloud management enabled`	Indicates whether cloud management is enabled. Values are: • `enabled` • `disabled` (default)

View support configuration

View the current support configuration information.

Format

```
/sys/support/config show
```

Example 1

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 enabled = yes
        Support proxy server address = 10.0.0.1
        Support proxy server port    = 1080
```

Example 2

The following command displays the support configuration:

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

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

1:     Support proxy server enabled               = no
       Support proxy server address               =
       Support proxy server port                  = 0
      Support proxy user name                    =
      Support proxy protocol                     = Unknown
      Automatic support contracts update enabled = no
      Cloud management enabled                   = no
```

Change support configuration

Change support configuration attributes.

Format

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

Action qualifiers

Qualifier	Description
`-enableSupportProxy`	Specifies whether to enable or disable the proxy server. Valid values are: - `yes` - `no`
`-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 is 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.
`-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.
-enableCloudMgmt	Specify whether sending data to CloudIQ is enabled on the system. Valid values are: • yes • no **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 -supportProxyProtocol http
```

```
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 11 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 • 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 Centralized ESRS

Centralized ESRS runs on a gateway server. When you select this option, your storage system is added to other storage systems in an ESRS cluster. The cluster resides behind a single common (centralized) secure connection between EMC servers and an off-array ESRS Gateway. The ESRS Gateway is the single point of entry and exit for all IP-based ESRS activities for the storage systems associated with the gateway.

The ESRS Gateway is a remote support solution application that is installed on one or more customer-supplied dedicated servers. The ESRS Gateway functions as a communication broker between the associated storage systems, Policy Manager and proxy servers (optional), and the EMC enterprise. Connections to the Policy Manager and associated proxy servers are configured through the ESRS Gateway interface along with add (register), modify, delete (unregister), and querying status capabilities that ESRS clients can use to register with the ESRS Gateway.

Note

To use Centralized ESRS, valid support credentials must be set.

The following table lists the attributes for Centralized ESRS:

Table 12 Centralized ESRS attributes

Attributes	Description
`Enabled`	Indicates whether the Centralized ESRS service is enabled. Valid values are: • `yes` • `no`
`Address`	Indicates the IP address of the Centralized ESRS server.
`Port`	Indicates the port number of the Centralized ESRS server.

View Centralized ESRS configuration

View details about the Centralized ESRS configuration.

Format

```
/sys/support/esrsc show
```

Example

The following command displays the Centralized ESRS configuration:

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

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

1:     Enabled = yes
       Address = 10.10.10.123
       Port    = 9443
```

Change Centralized ESRS configuration

Change the Centralized ESRS attributes.

Action qualifiers

Qualifier	Description
`-enable`	Specifies whether to enable or disable Centralized ESRS. Valid values are:

Qualifier	Description
	• yes • no **Note** If ESRS is disabled, other parameters cannot be changed.
-address	Specifies the IP address of the Centralized ESRS to which to be connected.
-port	Specifies the port number to be used to connect to the centralized ESRS.

Format

```
/sys/support/esrsc set -enable { yes | no } [ -address
<value> ] [ -port <value> ]
```

Example

The following command specifies the Centralized ESRS parameters:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsc
set -enable yes -address 10.10.22.22
```

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

Operation completed successfully.
```

Check Centralized ESRS network connection

Check Centralized ESRS network connectivity before configuring ESRS.

Check the network connectivity from Centralized ESRS to the EMC servers. If there is any failure, Centralized ESRS cannot be enabled.

Format

```
/sys/support/esrsc checkNetwork -address <value> [-port
<value>]
```

Action qualifier

Qualifier	Description
-address	Type the IP address of Centralized ESRS VE.
-port	Type the port number used for Centralized ESRS VE.

Example

This example shows when the network connectivity check for Centralized ESRS fails.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsc
checkNetwork -address 10.100.10.7
```

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

```
Operation failed. Error code: 0x6400be8

The centralized ESRS network connectivity check failed. Please
check your firewall configuration and whether the centralized ESRS
server is operating normally. (Error Code:0x6400be8)
```

Test Centralized ESRS

Once Centralized ESRS is already configured, you can use this command to test the connection between your system and the ESRS database. While the `checkNetwork` command will check your local network connectivity, this `test` command will check the connection back to Dell EMC.

Format

`/sys/support/esrsc test`

Example 1

The following example shows the results of running this command when Centralized ESRS is not yet configured.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsc
test
```

```
Operation failed. Error code: 0x6400c06
 Not supported since Centralized Secure Remote Support is not
enabled. (Error Code:0x6400c06)
```

Example 2

The following example shows when this command is run successfully.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsc
test
```

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

Operation completed successfully.
```

Note

A successful operation indicates that the test was executed successfully, not that the connection itself was successful. In other words, it indicates a Call Home was sent, but does not indicate whether it was received by the ESRS server. To check the status of the actual test, log into Service 360 to view recent Service Requests (SRs). If the call home was received by the ESRS server, the connection test will appear as an automatically-closed Call Home SR.

Manage Integrated ESRS (physical deployments only)

Note

This feature may not be available in your implementation.

Integrated ESRS runs directly on your storage system. When you configure this option, your storage system sets up a secure connection between itself and the Support Center. You can select one of the following remote service connectivity options for Integrated ESRS:

- Outbound/Inbound, which is the default, from the storage system to the Support Center and from the Support Center to the storage system for remote access using https.
- Outbound only from the storage system to the Support Center using https.

When you select the Outbound/Inbound option, the storage system sets up a secure connection between itself and the Support Center. This option enables remote service connectivity for dial out and dial in capabilities with the storage system. The connection from the storage system to a Policy Manager and any associated proxy servers (optional) must be configured through either Unisphere or the CLI.

When you select the Outbound only option, the storage system sets up a secure connection between itself and the Support Center. This option enables remote service connectivity for dial out only capabilities with the storage system.

Note

To use Integrated ESRS, valid support credentials must be set. Integrated ESRS is required to be enabled before you can configure a policy manager and any associated proxy servers.

The following table lists the attributes for Integrated ESRS:

Table 13 Integrated ESRS attributes

Attribute	Description
`Enabled`	Indicates whether the Integrated ESRS service is enabled. Valid values are: • `yes` • `no`
`EULA accepted`	Indicates whether the ESRS end user license agreement EULA has been accepted. Valid values are: • `yes`
`Site ID`	Indicates the assigned ID number for the location within your organization where the system is located.
`Type`	Specifies the Integrated ESRS type. Valid values are: • `oneWay` • `twoWay`

View Integrated ESRS configuration

View details about the Integrated ESRS configuration.

Format

`/sys/support/esrsi show`

Example

The following command displays the Integrated ESRS configuration:

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

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

1:     Enabled       = yes
       EULA accepted = yes
       Type          = Two way
```

Change Integrated ESRS configuration

Change the Integrated ESRS attributes.

Format

```
/sys/support/esrsi set {-enable {yes|no}|-acceptEula yes|-type
{oneWay|twoWay}}
```

Action qualifiers

Qualifier	Description
`-enable`	Specifies whether to enable or re-enable, or disable the ESRS. Valid values are: • `yes` • `no` **Note** If ESRS is disabled, other parameters cannot be changed.
`-acceptEula`	Specifies whether to accept the end user license. Valid value is: • `yes` **Note** If ESRS EULA is not accepted, nothing can be configured for the Integrated ESRS.
`-type`	Specifies which type of Integrated ESRS to use. Valid values are: • `oneWay` (Outbound only) • `twoWay` (Outbound/Inbound) (default)

Example

The following command specifies the Integrated ESRS parameters:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi set -acceptEula yes`

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

Operation completed successfully.
```

Check Integrated ESRS network connection

Check the network connectivity from the Integrated ESRS client to the EMC servers. If there is any failure, the Integrated ESRS cannot be enabled.

Format

`/sys/support/esrsi checkNetwork`

Example

The following command displays the network connectivity for Integrated ESRS:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi checkNetwork`

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

Operation failed. Error code: 0x6400bc8
 Remote Support cannot be enabled at this time, because the system
cannot contact some required EMC servers: esrghoprd02.emc.com:
443/8443,esrghoprd03.emc.com:8443/443. Please refer to online help
for this error code to resolve the issue. (Error Code:0x6400bc8)
```

Check support credential readiness for integrated ESRS

Before configuring ESRS, check that the support account credentials configured for your system are properly registered in the Online Support database.

Format

`/sys/support/esrsi checkSupportAccountReadiness`

Example 1

The following example shows that the command run successfully, where support credentials are properly configured.

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi checkSupportAccountReadiness`

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

Operation completed successfully.
```

Example 2

The following example shows the command fails because ESRS is already configured. The readiness check can only be performed before ESRS is configured. If ESRS was already successfully configured, your support credentials are successfully set up in the Online Support database.

Note

If you have an online support account, but your support credentials fail the readiness check, you may have a "lite" online support account that needs to be upgraded to a "full access" account. Refer to the *Unity Secure Remote Services Requirements and Configuration* guide for more information. If you already have a full access account, you may need to contact your service provider to resolve this issue.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi
checkSupportAccountReadiness
```

```
Operation failed. Error code: 0x6400b77
This operation can only be performed before ESRS is initially
configured. Refer to REST API or UEMCLI documentation for reference
(Error Code:0x6400b77)
```

Test Integrated ESRS

Once Integrated ESRS is already configured, you can use this command to test the connection between your system and the ESRS database. While the `checkNetwork` command will check your local network connectivity, this `test` command will check the connection back to Dell EMC.

Format

```
/sys/support/esrsi test
```

Example 1

The following example shows the results of running this command when Integrated ESRS is not yet configured.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi
test
```

```
Operation failed. Error code: 0x6400bad
 Not supported since Integrated Secure Remote Support is not
enabled. (Error Code:0x6400bad)
```

Example 2

The following example shows when this command can be executed successfully.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi
test
```

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

Operation completed successfully.
```

Note

A successful operation indicates that the test was executed successfully, not that the connection itself was successful. In other words, it indicates a Call Home was sent, but does not indicate whether it was received by the ESRS server. To check the status of the actual test, log into Service 360 to view recent Service Requests (SRs). If the call home was received by the ESRS server, the connection test will appear as an automatically-closed Call Home SR.

Request access code for Integrated ESRS

Request an access code for Integrated ESRS. This access code will be emailed to the email account user. The access code will only be valid for 30 minutes. This process adds an extra level of authentication and helps to ensure that you are the correct user and authorized to enable ESRS on the storage system.

Format

```
/sys/support/esrsi requestAccessCode
```

Example

The following command sends a request for an access code as part of the email verification process for Integrated ESRS:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi
requestAccessCode
```

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

1:     Recipient email address = sxxxxxxxxxx@mail.com
```

Validate access code for Integrated ESRS

Validate the access code for Integrated ESRS that was received by email to the email account user. The received access code will only be valid for 30 minutes.

Format

```
/sys/support/esrsi validateAccessCode -accessCode <value>
```

Example

The following command displays the response to validating the access code part of the email verification process:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi
validateAccessCode -accessCode 76507252
```

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

Operation completed successfully.
```

Manage Policy Manager

The Policy Manager is optional and is installed on a customer supplied server or servers. It enables customizable control of remote access to customer devices and maintains an audit log of remote connections. When the ESRS server retrieves a remote access from the EMC Enterprise, the access is controlled by the policies configured on the Policy Manager and are enforced by the ESRS server.

A proxy server can be configured for the server on which the Policy Manager is installed to connect to the Internet. The proxy server configured for the Policy Manager is called a Policy Manager Proxy.

Note

Integrated ESRS is required to be enabled before you can configure a Policy Manager and any associated proxy servers.

The following table lists the attributes for a Policy Manager and proxy server:

Table 14 Policy Manager and proxy server attributes

Attribute	Description
`Enabled`	Indicates whether the policy manager is enabled or not. Valid values are: • `yes` • `no`
`Address`	Policy manager name or IP address
`Port`	Policy manager port number
`Protocol`	Protocol used for communication with the policy manager. Valid values are: • `http` • `https` (default)
`SSL strength`	The ESRS Policy Manager SSL strength (applicable only when protocol is HTTPS). Valid values are: • `high` (default) • `medium` • `low`
`Proxy enabled`	Indicates whether the policy manager proxy is enabled or not. Valid values are: • `yes` • `no`
`Proxy address`	Name or IP address of the proxy server used by the policy manager
`Proxy port`	Port of the proxy server used by the policy manager
`Proxy username`	Name of the account on the policy proxy server
`Proxy password`	Password of the account on the policy proxy server

Table 14 Policy Manager and proxy server attributes (continued)

Attribute	Description
`Proxy protocol`	Protocol used for communications with the policy proxy server. Valid values are: • `http` • `socks` (default)

View Policy Manager and proxy server configuration

View details about the Policy Manager and proxy server configuration.

Format

```
/sys/support/esrsi/policymgr show
```

Example

The following command displays the configuration of the Integrated ESRS policy manager server:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi/
policymgr show -detail
```

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

1:      Enabled          = no
        Address          =
        Port             = 0
        Protocol         =
        SSL strength     =
        Proxy enabled    = no
        Proxy address    =
        Proxy port       = 0
        Proxy user name  =
        Proxy protocol   =
```

Change Policy Manager and proxy server configuration

Change the Policy Manager and proxy server attributes.

Action qualifiers

Qualifier	Description
`-enable`	Specifies whether to enable or disable the ESRS policy manager. Valid values are: • `yes` • `no` **Note** If the ESRS policy Manager is disabled, other policy manager parameters cannot be changed.

Qualifier	Description
-address	Specifies the policy manager address to be configured for Integrated ESRS.
-port	Specifies the policy manager server port number to be configured for Integrated ESRS.
-protocol	Specifies the protocol to be used by the policy manager server.
-sslStrength	Specifies the ESRS Policy Manager SSL strength (applicable only when the protocol is HTTPS). Valid values are: • high • medium • low
-enableProxy	Specifies to enable the policy manager proxy. Valid values are: • yes • no **Note** If the ESRS Policy Manager is disabled, other policy manager proxy server parameters cannot be changed.
-proxyAddr	Specifies the policy proxy server address.
-proxyPort	Specifies the policy proxy port number.
-proxyUser	Specifies the user name of the account on the policy manager proxy server.
-proxyPasswd	Specifies the password of the account on the policy manager proxy server.
-proxyProtocol	Specifies the protocol to be used by the policy manager proxy server.

Format

```
/sys/support/esrsi/policymgr set [ -enable { yes | no } ] [ -
address <value> ] [ -port <value> ] [ -protocol { http |
https } ] [ sslStrength { high | medium | low } ] [ -
enableProxy { yes | no } ] [ -proxyAddr <value> ] [ -proxyPort
<value> ] [ -proxyUser <value> { -proxyPasswd <value> | -
proxyPasswdSecure } ] [ -proxyProtocol { http | socks } ]
```

Example

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi/
policymgr set -enable no
```

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

Operation completed successfully.
```

Manage Connect Home

Configure Connect Home to send system information directly to support when critical alerts occur.

Connect Home uses SMTP (Simple Mail Transport Protocol) to automatically email system information directly to support. These emails contain system event and error histories that can be used by support for diagnosing and troubleshooting issues.

Table 15 Connect Home attributes

Attribute	Description
`Enabled`	Indicates whether Connect Home is enabled. Valid values are: • `yes` • `no`
`SMTP server`	The IP address of the SMTP server configured for Connect Home.
`E-mail from address`	The email address from which Connect Home emails are sent to support.
`E-mail to address`	The destination email address to which Connect Home emails are sent.

View Connect Home

This command shows the Connect Home configuration settings.

View the current Connect Home configuration settings.

Format

```
/sys/support/connecthome show
```

Example

The following command shows the configuration details for Connect Home.

`uemcli -d 10.0.0.1 -u admin -p Password /sys/support/connecthome show -detail`

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

1:     Enabled             = yes
       SMTP server         = 10.10.10.123
       E-mail from address = bs-xxxx@emc.com
       E-mail to address   = emailalertesg@emc.com
```

Change the Connect Home configuration settings

This command changes the configuration settings for Connect Home.

Change the configuration settings for Connect Home.

Format

```
/sys/support/connecthome set [-enable {yes | no}] [ -smtpServer
<value>] [-emailFromAddr <value>]
```

Action qualifiers

Qualifier	Description
`-enable`	Specify whether to enable Connect Home. Valid values are: • `yes` • `no`
`-smtpServer`	Specify the IP address of the SMTP server that Connect Home will use to send emails.
`-emailFromAddr`	Specify the email address from which Connect Home emails will be sent to support. If not specified, a default value formatted as *<arrayname>*@emc.com will be used.

Example

This example enables Connect Home and specifies that it will use SMTP server 10.10.22.22.

```
uemcli -d 10.0.0.1 -u local/joe -p Password /sys/support/connecthome
set –enable yes –smtpServer 10.10.22.22
```

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

Operation completed successfully.
```

Test Connect Home

This command tests a successful Connect Home email alert transmission.

Test whether Connect Home can successfully send an email alert to support using the specified SMTP server.

Format

```
/sys/support/connecthome test
```

Example

This example shows the results of a test email alert using the specified Connect Home configuration settings.

```
uemcli -d 10.0.0.1 -u local/joe -p Password /sys/support/connecthome
test
```

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

Operation completed successfully.
```

Manage user roles

View the supported roles of users on the system, as well as the types of actions each type of user can perform.

The following table lists the attributes for user roles:

Table 16 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. • `securityadministrator`— Security administrator role: Can view system and storage status information but perform only security related tasks. Cannot perform any operations. • `vmadmin`— VMware administrator role: Used only for adding the system as a VASA provider in vCenter.
`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.

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

Qualifier	Description
	• storageadmin — Storage Administrator role • operator — Operator role (view only) • securityadministrator — Security Administrator role • vmadmin— VMware Administrator (used only to register the system as a VASA provider in vCenter)

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 -detail

```
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.

4:      Name        = securityadministrator
        Description = User is allowed only to perform security tasks 
and is able to see all storage system data, but cannot perform any 
operations.

5:      Name        = vmadmin
        Description = Can only be used to establish a VASA 
connection from vCenter to the storage system.
```

Manage user accounts

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. When users connect to the system through the CLI or Unisphere UI, the system prompts them to type their username and password to gain access.

Table 17 User account attributes

Attributes	Description
ID	Identifier of the specific user account.
Name	Account name.
Role	The role type of the user account.
Type	The account type (scope). Values are:

Table 17 User account attributes (continued)

Attributes	Description
	- local - ldapuser - ldapgroup
Password	Local account password.
Password expiration status	Information about when the account password will expire. Values are: - *<value>* days remaining - Expired - An empty value, which means the password does not expire for that specific user account. For example, user accounts with the account type of ldapuser or ldapgroup.

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, specify only the username, do not include the domain name. **NOTICE** The LDAP user or group name is case sensitive; that is, use the same case as the LDAP user or group that is specified in the LDAP server.
-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:

Qualifier	Description
	• 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.
`-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) • `securityadministrator` — Security Administrator • `vmadmin`— VMware Administrator The `/user/role show -detail` command returns a list of all available user roles. Table 16 on page 78 provides a detailed 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.

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>*] [-locked {yes | no}]

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.

Qualifier	Description
	Note You must be an administrator to use this qualifier.
`-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) • `securityadministrator` — Security Administrator • `vmadmin`— VMware Administrator The `/user/role show -detail` command returns a list of all available user roles. Table 16 on page 78 provides a description of each user role.
`-locked`	Specifies whether to lock or unlock the user account. Valid values are: • `yes`--locks the user account. • `no`--unlocks the user account. **Note** This option can only be set by users who have either the administrator or security administrator role, and only on STIG-enabled systems.

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
```

Manage user account settings

Manage the detailed account settings for users on the system.

Note

This command is available only for STIG-enabled systems.

Table 18 User account settings attributes

Attributes	Description
`Enabled`	Indicates whether or not the user account settings feature is enabled. Values are: - `yes` - `no` **Note** When this value is `yes`, but the detailed account settings are not specified, the "Default enabled value" for each setting, as specified below, is used. When this value is `no`, the "Disabled value" for each setting is used.
`Password minimum size`	Minimum number of characters for a password. Value range is `8-40`. Default values are: - Default enabled value: `15` - Disabled value: `8`

Table 18 User account settings attributes (continued)

Attributes	Description
`Number of previous passwords`	Indicates the number of past passwords that cannot be reused until the cycle has reset. Value range is `3-12`. Default values are: - Default enabled value: `5` - Disabled value: `3`
`Password period`	The time period (in days) a password is valid for before it expires. Value range is `1-180` days. An empty value indicates the password does not expire. Default values are: - Default enabled value: `60` - Disabled value: no expiration (empty)
`Maximum failed logins`	The number of consecutive failed login attempts allowed within the failed login period before the account is locked. An empty value indicates that there is no limit. Value range is `1-10`. Default values are: - Default enabled value: `3` - Disabled value: no limit (empty) Note `Maximum failed logins`, `Failed login period`, and `Account lockout period` must either be all empty or they must all have a value.
`Failed login period`	The time period (in seconds) during which the failed login attempts are tracked and considered, thus counting toward the maximum failed logins before lockout. Value range is `1-3600` seconds. An empty value indicates that the failed login period is not tracked. Default values are: - Default enabled value: `900` - Disabled value: no failed login period tracking (empty) If the maximum failed logins is not met during the `Failed login period`, the `Maximum failed logins` count will reset. Note `Failed login period`, `Maximum failed logins`, and `Account lockout period` must either be all empty or they must all have a value.

Table 18 User account settings attributes (continued)

Attributes	Description
`Account lockout period`	The time period (in seconds) for which an account will be locked before the user can attempt to login again. Value range is `1-86400` seconds. Default values are: - Default enabled value: `3600` - Disabled value: account never locks (empty). **Note** `Account lockout period`, `Maximum failed logins`, and `Failed login period` must either be all empty or they must all have a value.
`Session idle timeout`	The time period (in seconds) of idle activity, after which the login session will time out. Value range is: `1-3600` seconds. Default values are: - Default enabled value: `600` - Disabled value: `3600` **Note** An empty value means the session will not timeout due to being idle.
`Default admin lockout enabled`	Indicates whether account lockout is enabled for admin users. Values are: - `yes` - `no` Default values are: - Default enabled value: `no` - Disabled value: `no`

Configure user account settings

Configure the user account settings for a STIG-enabled system. If the `-enabled` option is `yes`, all other subsequent options can be specified. If the subsequent options are not specified when user account settings `-enabled` is set to `yes`, the default enabled value specified below will be used. The disabled value for these options when user account settings `-enabled` is set to `no` are detailed in the attributes table in Manage user account settings on page 84.

Note

This command is not valid for systems that do not have STIG enabled.

Format

```
/user/account/settings set [-enabled {yes | no}] [-
passwdMinSize <value>] [-passwdCount <value>] [{-passwdPeriod
<value> | -noPasswdPeriod}] [{-maxFailedLogins <value> | -
noMaxFailedLogins}] [{-failedLoginPeriod <value> | -
noFailedLoginPeriod}] [{-lockoutPeriod <value> | -
noLockoutPeriod | -manualUnlock}] [{-sessionIdleTimeout <value>
| -noSessionIdleTimeout}] [-defaultAdminLockoutEnabled {yes |
no}]
```

Action qualifiers

Qualifier	Description
-enabled	Specifies whether to enable or disable user account settings. Valid values are: • yes • no
-passwdMinSize	Specifies the minimum number of characters for a password. Value range is 8-40. If not specified, user account setting default enabled value is 15.
-passwdCount	Specifies the number of passwords that cannot be reused. Valid range: 3 -12. If not specified, user account setting default enabled value is 5.
-passwdPeriod	Specifies the time period (in days) for which a password is valid before it expires. Value range is 1-180 days. If neither this value nor -noPasswdPeriod is specified, user account setting default enabled value is 60. **Note** This setting is not applicable to local admin user accounts.
-noPasswdPeriod	Specifies that the password does not have an expiry period for local user accounts.
-maxFailedLogins	Specifies the number of consecutive failed login attempts allowed within the failed login period before the account is locked. Value range is 1-10. If neither this value nor -noMaxFailedLogins is specified, user account setting default value is 3. **Note** If this option is specified, the -failedLoginPeriod and -lockoutPeriod options must also be specified.
-noMaxFailedLogins	Specifies that there is no maximum limit on the number of consecutive failed login attempts. **Note** If this option is specified, the -noFailedLoginPeriod and -noLockoutPeriod options must also be specified.

Qualifier	Description
-failedLoginPeriod	Specifies the time period (in seconds) during which the failed login attempts are tracked and considered, thus counting toward the maximum failed logins before lockout. Value range is 1-3600 seconds. If neither this value, nor -noFailedLoginPeriod is specified, user account setting default enabled value is 900. **Note** If this option is specified, the -maxFailedLogins and -lockoutPeriod options must also be specified. If the maximum failed logins is not met during the Failed login period, the Maximum failed logins count will reset.
-noFailedLoginPeriod	Specifies that the number of consecutive failed login attempts within a given time period is not being tracked. **Note** If this option is specified, the -noMaxFailedLogins and -noLockoutPeriod options must also be specified.
-lockoutPeriod	Specifies the time period (in seconds) for which an account will be locked before the user can attempt to login again. Value range is 1-86400 seconds. If neither this value, nor -noLockoutPeriod is specified, the user account settings default enabled value is 3600. **Note** If this option is specified, the -maxFailedLogins and -failedLoginPeriod options must also be specified.
-noLockoutPeriod	Specifies that local user accounts will not be locked due to meeting the number of -maxFailedLogins within the -failedLoginPeriod. **Note** If this option is specified, the -noMaxFailedLogins and -noFailedLoginPeriod options must also be specified.
-manualUnlock	Specifies that the account will remain locked until manually unlocked by an administrator.
-sessionIdleTimeout	Specifies the time period (in seconds) of idle activity, after which the login session will time out. Value range is: 1-3600 seconds. If neither this value, nor -noSessionIdleTimeout is specified, the user account settings default enabled value is 600.
-noSessionIdleTimeout	Specifies that the session will never time out due to being idle.

Qualifier	Description
-defaultAdminLockoutEnabled	Specifies whether account lockout is enabled for admin users. Values are: • yes • no If this value is not specified, the user account settings default enabled value is no.

Example 1

The following command enables the user account settings with all default enabled values set when transitioning from a disabled state:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account/settings set -enabled yes
```

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

Operation completed successfully.
```

Example 2

The following command disables the user account settings, which reverts the account settings back to the original values from before the settings were enabled:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account/settings set -enabled no
```

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

Operation completed successfully.
```

View user account settings

View the account setting details of all users on the system.

Format

```
/user/account/settings show
```

Example

Displays the user account settings for all users on the system:

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

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

1:    Enabled                         = yes
      Password minimum size           = 15
      Number of previous passwords    = 5
      Password period                 = 60
```

```
       Maximum failed logins          = 3
       Failed login period            = 900
       Account lockout period         = 3600
       Session idle timeout           = 600
       Default admin lockout enabled = no
```

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 19 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.

Qualifier	Description
`-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 -d 10.0.0.1 -u Local/joe -p MyPassword456! /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 -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/account
delete
```

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

Operation completed successfully.
```

Manage system limits

This CLI command shows limits of the system and various storage resources.

System limits display the size, capacity, and count limits of various system components or storage resources. Some of these limits are associated with alert thresholds. If this threshold is exceeded, the system will generate an alert. Certain limits are license dependent.

Table 20 System limit attributes

Attribute	Description
`ID`	Limit identifier.
`Name`	Limit name.
`Description`	Limit description.
`Limit value`	Upper boundary of the limit that cannot be exceeded.

Table 20 System limit attributes (continued)

Attribute	Description
`Threshold value`	Threshold of the specified limit above which the system will generate an alert.
`License`	License identifier related to the given limit. Some system limits depend on the type of license installed.

View system limits

This command allows you to view system limits, limit thresholds that trigger related alerts, and limits that are based on product feature licenses.

View details about system limits.

Format

/sys/limits [{-id *<value>* | -license *<value>*}] show

Object qualifier

Qualifier	Description
`-id`	Type the identifier of the limit.
`-license`	Type a specified license for which to display associated limits.

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/limit show -detail

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

1:     ID              = Limit_Pool_MaxCapacityInTotal
       Name            = Max Storage Capacity
       Description     = The maximum allowed capacity of all
storage pools in total.
       Limit value     = 17179869184 (16.0 TB)
       Threshold value = 15032385536 (14.0 TB)
       License         = STORAGE_CAPACITY_LIMIT

2:     ID              = Limit_Pool_MaxCount
       Name            = Max Storage Pool Count
       Description     = The maximum allowed number of storage
pools on the system.
       Limit value     = 10
       Threshold value = 8
       License         =

3:     ID              = Limit_VirtualDisk_MinSize
       Name            = Min Virtual Disk Size
       Description     = The minimum allowed size of a virtual disk.
       Limit value     = 10737418240 (10.0 GB)
```

```
        Threshold value =
        License         =
```

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 29 provides details on all available switches. The following table lists and describes the attributes for product licenses.

Table 21 License attributes

Attribute	Description
`ID`	License identifier.
`Name`	Name of the license.
`Description`	Description of the license.
`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 View the switches on page 29, for health information details.

View licenses

View details about installed licenses.

Note

The show action command on page 23 explains how to change the output format.

Format

```
/sys/lic [-id <value>] show
```

Object qualifier

Qualifier	Description
-id	Identify the license.

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:      ID            = ISCSI
        Name          = Internet Small Computer System Interface
(iSCSI)
        Description   = This license enables you to use the iSCSI
        protocol for block storage.
        Installed     = yes
        Version       = 1.1
        Issued        = 2009-11-09
        Expires       = 2010-11-09
        Health state  = OK (5)

2:      ID            = CIFS
        Name          = Common Internet File System (CIFS)
        Description   = This license enables you to configure and
        manage file shares that are exposed using the CIFS protocol.
        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

The show action command on page 23 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 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 22 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. Valid values are: • `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 maximum of five remote hosts. Create a setting for remote logging for each host that specifies the following:

- The facility that will generate the log messages.
- The network name or IP address of the remote host that will receive the log data.
- The severities that will be sent to the remote host.

Each 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. For the default configuration, the system transfers log information on port 514 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.

View event logs and alerts on page 638 explains viewing details about current logs and alerts on the system.

The following table lists the attributes for remote system logging.

Table 23 Remote logging attributes

Attribute	Description
`ID`	Remote system log identifier.
`Enabled`	Indication of whether remote logging is currently enabled. Valid values are (case-insensitive): • `yes` • `no`
`Host`	IP address or network name of the remote host.
`Port`	Port number on the remote host. Default is *514*.
`Protocol`	Protocol for transferring the log. Valid values are (case-insensitive): • `tcp` • `udp`
`Facility`	Facility that will process the log. Value is one of the following (case-insensitive): • `KERN` - Kernel messages. • `USER` - User-level messages. • `Syslog` - Message generated internally by syslogd (default).
`Severity`	Least severities that will be sent to the remote host. Valid values are (case-insensitive): • `emergency` • `alert` • `critical` • `error` • `warning` • `notice` • `info` • `debug`

Create remote logging configuration

Create remote logging configuration.

Format

```
/sys/rlog create [-enabled {yes|no}] [-host <value>] [-port
<value>] [-protocol {udp|tcp}] [-facility {KERN | USER |
Syslog}] [-severity {emergency | alert | critical | error |
warning | notice | info | debug}]
```

Object qualifier

Qualifier	Description
`-enabled`	Specify to enable remote system logging. Valid values are (case-insensitive): • `yes` • `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 address>* • *<IPv6 address>* • *<network name>* **Note** The new IP address and port combination cannot be identical to any existing remote host address.
`-port`	Type the port number on which the host will receive the transferred log information. Default is *514*.
`-protocol`	Type the protocol for transferring the log files. Valid values are (case-insensitive): • `tcp` • `udp`
`-facility`	Type the facility that will process the log files. Value is one of the following (case-insensitive): • `KERN`—Kernel messages. • `USER`—User-level messages. • `Syslog` (default)—Message generated internally by syslog.
`-severity`	Type the least severities of the log files that will be sent to the remote host. Value is one of the following (case-insensitive): • `emergency` • `alert` • `critical`

Qualifier	Description
	- `error` - `warning` - `notice` - `info` - `debug` **Note** For example, `debug` is the default severity. When it is typed, all user/audit logs are sent to the remote host. When `emergency` is typed, only logs of emergency severity are sent to the remote host.

Example

The following command configures remote system logging with these settings:

- Remote target host is 10.10.10.10
- Uses host port 8181.
- Uses protocol `tcp`.
- Uses the `syslog` facility.
- Uses the `notice` severity.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/rlog set –
enabled yes –host 10.10.10.10 –port 8181 –protocol TCP -facility
syslog -severity notice
```

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

Operation completed successfully.
```

View settings for remote logging

View remote logging settings.

Format

```
/sys/rlog show
```

Object qualifier

Qualifier	Description
`-id`	Type the ID that identifies the remote host. Optional if there is only one remote host configured.

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:      ID        = RemoteSysLogPort_0
        Enabled   = yes
        Host      = 10.0.0.1
        Port      = 514
        Protocol  = UDP
        Facility  = KERN
        Severity  = DEBUG
```

Change remote logging configuration

Update remote logging configuration with new settings.

Format

```
/sys/rlog [-id <value>] set [-enabled {yes|no}] [-host <value>]
[-port <value>] [-protocol {udp|tcp}] [-facility {KERN | USER |
Syslog}] [-severity {emergency | alert | critical | error |
warning | notice | info | debug}]
```

Object qualifier

Qualifier	Description
`-id`	Type the ID that identifies the remote host. Optional if there is only one remote host configured.

Action qualifier

Qualifier	Description
`-enabled`	Specify to enable remote system logging. Valid values are (case-insensitive): • `yes` • `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 address>* • *<IPv6 address>* • *<network name>* **Note** The new IP address and port combination cannot be identical to any existing remote host address.
`-port`	Type the port number on the remote host. Default is *514*.
`-protocol`	Type the protocol for transferring the log files. Valid values are (case-insensitive): • `tcp`

Qualifier	Description
	- udp
-facility	Type the facility that will process the log files. Value is one of the following (case-insensitive): - KERN - Kernel messages. - USER - User-level messages. - Syslog (default) - Message generated internally by syslog.
-severity	Type the least severities of the log files that will be sent to the remote host. Value is one of the following (case-insensitive): - emergency - alert - critical - error - warning - notice - info - debug **Note** For example, debug is the default severity. When it is typed, all user/audit logs are sent to the remote host. When emergency is typed, only logs of emergency severity are sent to the remote host.

Example

The following command configures remote system logging with these settings:

- Remote target host is 10.64.74.12
- Uses host port 514.
- Uses protocol udp.
- Uses the KERN facility.
- Uses the critical severity.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/rlog set –
enabled yes –host 10.64.74.12 –port 514 –protocol UDP -facility KERN -
severity critical
```

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

ID = RemoteSysLogPort_0
Operation completed successfully.
```

Delete remote logging configuration

Delete a remote logging configuration.

NOTICE

If only one remote destination exists, you are not allowed to delete it.

Format

```
/sys/rlog -id <value> delete
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the remote host to delete.

Example

The following command deletes remote host RemoteSysLogPort_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/rlog -id
RemoteSysLogPort_1 delete
```

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

Operation completed successfully
```

Manage system certificates

Interface to manage certificates for different components on the storage system.

The following table lists the attributes for certificates:

Table 24 Certificate attributes

Attribute	Description
`ID`	Certificate identifier.
`Type`	Certificate type. Valid certificate types are: - `CA` - `Server` - `Client` - `TrustedPeer`
`Service`	Service with which the certificate is associated. The services supported are: - `Mgmt_LDAP` - `Mgmt_KMIP` - `VASA_HTTP`
`Scope`	Scope of the certificate. The certificate can have local or global scope. If global, there will be no value. If local, value will be the ID of the scope. For example, if the scope of the certificate associated with `Mgmt_LDAP` service is NAS server nas01, the value of the property would be nas01.

Table 24 Certificate attributes (continued)

Attribute	Description
`Trust anchor`	Indicates whether the certificate is trusted as end-of-chain for peer certificate verification. Valid values are: • `yes` • `no`
`Version`	Certificate version.
`Serial number`	Certificate serial number.
`Signature algorithm`	Certificate signature algorithm.
`Issuer name`	Name of the certificate issuer.
`Valid from`	Date and time when the certificate became valid.
`Valid to`	Date and time when the certificate will expire.
`Subject`	Certificate subject.
`Subject alternative name`	Certificate subject alternative name.
`Public key algorithm`	Certificate public key algorithm.
`Key length`	Certificate key length.
`Thumbprint algorithm`	Certificate thumbprint algorithm.
`Thumbprint`	Certificate thumbprint.
`Private key available`	Indicates whether the certificate has an associated private key. Based on availability, valid values are: • `yes` • `no`

View certificates information

View details about a certificate.

Format

```
/sys/cert [ -type { CA | Server | Client | TrustedPeer } ] [ -
service { Mgmt_LDAP | Mgmt_KMIP | VASA_HTTP } [ -scope
<value> ] ] [ -id <value> ] show
```

Object qualifier

Qualifier	Description
`-id`	Identifies the certificate.
`-type`	Identifies the type of certificate.

Qualifier	Description
-service	Identifies the Service. Valid values are: - Mgmt_LDAP - Mgmt_KMIP - VASA_HTTP
-scope	Identifies the scope of the certificate.

Example

The following command displays a VASA HTTP certificate information:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/cert -id vasa_http-vc1-cacert-1 show -detail

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

1:    ID                        = vasa_http-vc1-cacert-1
      Type                      = CA
      Service                   = VASA_HTTP
      Scope                     =
      Trust anchor              = no
      Version                   = 2
      Serial number             = 04:00:00:00:00:01:21:58:53:08:A2
      Signature algorithm       = SHA256WithRSAEncryption
      Issuer name               = CN = GlobalSign O = GlobalSign OU
= GlobalSign Root CA - R3
      Valid from                = 2009-03-18 10:00:00
      Valid to                  = 2029-03-18 10:00:00
      Subject name              = CN = GlobalSign O = GlobalSign OU
= GlobalSign Root CA - R3
      Subject alternative name =
      Public key algorithm      = RSA
      Key length                = 2048
      Thumbprint algorithm      = SHA1
      Thumbprint                = d6 9b 56 11 48 f0 1c 77 c5 45 78
c1 09 26 df 5b 85 69 76 ad
      Private key available     = no
```

Delete system certificate

Deletes an X509 certificate.

Format

`/sys/cert -id <value> delete`

Object qualifier

Object	Description
-id	Identifies the certificate.

Example

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/cert -id
vasa_http-vc1-servercert-1 delete
```

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

Operation completed successfully.
```

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 108 explains how to set up task rules. Manage snapshots on page 532 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 25 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 108 provides details about schedule rules.
`Sync replicated`	The state indicating to the user whether the schedule is synchronously replicated to the remote system. Value is one of the following: • `no`— The schedule is created locally and will not be replicated. • `yes`— The schedule is in sync with the remote system.
`Last modified time`	Last modified time of the schedule.

View protection schedules

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

Note

The show action command on page 23 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
        Sync replicated = no

2:      ID             = DefaultProtectionID
        Name           = Default Protection
        Type           = System
        Rules          = RULE_3
        Sync replicated = no

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

Delete protection schedules

Delete a user-defined protection schedule. You cannot delete a system-defined schedule or schedules that are associated or assigned to storage resources.

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 106 explains how to view and delete protection schedules.

The following table lists the attributes for task rules.

Table 26 Task rule attributes

Attribute	Description
`ID`	ID of the rule.
`Type`	Type of rule, which specifies when a task executes. Valid values are: • `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. Valid values are: • `yes` — The system can delete the snapshot automatically.

Table 26 Task rule attributes (continued)

Attribute	Description
	- `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. Valid values are: - `ckpt` — The snapshot is a read-only checkpoint - `share` — The snapshot is set to read/write for users to create CIFS (SMB) shares of NFS exports.

Create task rules

Create a task rule and add to an existing schedule. If a schedule does not exist, a new one is created.

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}] [-
syncRep {yes | no}]
```

Action qualifiers

Qualifier	Description
`-schedId`	Type the ID of an existing protection schedule to which to assign the rule. View protection schedules on page 106 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. Valid values are: - `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. Supports up to two specified hours. - `daysinterval` — Task executes on an interval of the specified number of days and, optionally, on a specific hour of each specified day.

Qualifier	Description
	- `weekdayslist`— Task executes on the specified days of the week or on a specific hour of each specified day. Supports up to seven specified values, including all the days in a week. - `monthdayslist`— Task executes each month on a specified day and time. Supports one day value only.
`-every` (used with `-type`)	If the value of `-type` is `hoursinterval` or `daysinterval`, type the time interval when the task will execute. Valid values are: - `hoursinterval` — Number of hours within the range 1 - 24. - `daysinterval` — Number of days within the range 1 - 31.
`-hours` (used with `-type`)	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` (used with `-type`)	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`. Valid values are: - `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` (used with `-type`)	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: - `weekdayslist`— Type a comma-separated list of the days of the week. Valid values are: ▪ `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.

Qualifier	Description
	Note For `monthdayslist`, you can specify only one 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 - 8760. ■ `days` — Number of days within the range 1 - 365. - *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. Valid values are: - `yes` (default) - `no`
`-access`	Specify whether the snapshot is a read-only checkpoint, or read/write for CIFS (SMB) shares or NFS exports. Valid values are: - `ckpt` (default) - `share`
`-syncRep`	Specify whether this schedule is synchronously replicated. All changes done to the replicated schedule on the local system apply to the remote system automatically and conversely. Valid values are: - `yes` - `no` **Note** If a synchronous remote connection is established, the default value is `yes`, otherwise it is `no`.

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 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 "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 23 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 8:30, 20:30
       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 27 Jobs attributes

Attribute	Description
`ID`	Job identifier.
`Type`	Job type. Value is one of the following: - `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`
`Result desciption`	Describes the result of the step.
`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.
`Associated object`	Object or storage resource affected by the job. Only one object is associated with each job. Format is shown as: `<id> (<object type>)`

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.

Qualifier	Description
`-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 1

The following command displays a list of all jobs:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /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%
```

Example 2

The following command displays a list of all jobs:

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

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

1:    ID                    = N-11
      Type                  = Storage resource provisioning
      Title                 = Create storage resource
      State                 = Completed
      Result description    = Success
      User                  = Local/admin
      Step                  =
      Start time            = 2016-06-17 09:47:36
      Elapsed time          = 1m 26s
      Estimated time left   =
      Percent complete      = 100%
      Associated object     = fs_3 (/stor/prov/fs)
```

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 -d 10.0.0.1 -u Local/joe -p MyPassword456! /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 -d 10.0.0.1 -u Local/joe -p MyPassword456! /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 -d 10.0.0.1 -u Local/joe -p MyPassword456! /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 28 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.
`Rollback result description`	The error message of the rollback.
`Details`	Additional information. Format: key: "value", key: "value",...
`Associated object`	Object or storage resource affected by the job. Only one object is associated with each job step. Format is shown as: `<id> (<object type>)`

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 1

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
```

Example 2

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

uemcli /sys/task/job/step -jobId N-11 show -detail

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

1:    Title                        = Create storage resource
      Status                       = Completed
      Execution result code        = 0
      Execution result description =
      Rollback result code         = 0
      Rollback result description  =
      Details                      = ID: "res_3"; Name: "testFS3"
      Associated object            =

2:    Title                        = Create file system
      Status                       = Completed
      Execution result code        = 0
      Execution result description =
      Rollback result code         = 0
      Rollback result description  =
      Details                      = ID: "fs_3"; Name: "testFS3"
      Associated object            = fs_3 (/stor/prov/fs)

3:    Title                        = Add filesystem to storage
resource
      Status                       = Completed
      Execution result code        = 0
      Execution result description =
      Rollback result code         = 0
      Rollback result description  =
      Details                      = ID: "res_3, fs_3"
      Associated object            =
```

CHAPTER 3

Configure Network Communication

This chapter contains 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 SMB 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 (SMB), Linux/UNIX network shares, 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 SMB 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 29 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.
`Tenant`	Identifier and name of the tenant.
`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 network

Table 29 NAS server attributes (continued)

Attributes	Description
	interfaces on page 213 explains how to configure network interfaces on the system. **Note** It is allowable to remove the last interface of the server.
`CIFS enabled`	Indicates whether SMB file systems are enabled on the NAS server. Value is yes or no. Default is no. SMB file systems provide support for SMB 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: • `local` • `nis` • `ldap` • `localThenNis` • `localThenLdap` • `none` (default) **Note** A value other than the default is required for accurate multiprotocol files sharing between Unix and Windows users.
`Auto user mapping enabled`	Applies when multiprotocol sharing mode is enabled. Indicates whether a Windows user who is not mapped to a known Unix/ Linux username is allowed to access the NAS server's files. • `yes`— The system generates an internal UID for the Windows user and allows access to the NAS server's files through Windows. • `no` (default)— The Windows authentication fails unless there is a default Unix username configured.
`Default Unix username`	Default Unix user name or Unix ID that grants file access in the multiprotocol sharing mode. This user name is used for Windows users when the corresponding Unix/Linux user name is not found by the mapping mechanism. The Unix ID format is @uid=xxxx,gid=yyyy@, where xxxx and yyyy are the decimal numerical values of the UID and the primary GID, respectively. When using this ID, the user does not need to be defined in the UDS.

Table 29 NAS server attributes (continued)

Attributes	Description
`Default Windows username`	Default Windows user name that grants file access in the multiprotocol sharing mode. This user name is used for Unix users when the corresponding Windows user name is not found by the mapping mechanism.
`Replication type`	Indicates in what asynchronous replication this NAS Server is participating. Valid values are: • `none` • `local` • `remote`
`Synchronous replication type`	Indicates in what synchronous replication this NAS Server is participating. Valid values are: • `none` • `remote`
`Replication destination`	Indicates whether the NAS server is a replication destination. Valid values are: • `yes` • `no` **Note** This attribute does not apply to the replication status of related file systems. Use the `stor/prov/fs show` command to view the replication status of file systems.
`Backup only`	Indicates whether the NAS server is used as backup. This attribute reflects that the NAS server cannot be the production site. This means both planned failover and unplanned failover are disallowed in the backup only NAS server associated replication session.
`Migration destination`	Indicates whether the NAS server is a destination for a NAS import session. Valid values are: • `yes` • `no`
`Username translation`	Indicates whether a Unix to/from Windows user name mapping is enabled. Valid values are: • `yes` • `no`
`Packet Reflect enabled`	Indicates whether the reflection of outbound (reply) packets through the same interface that inbound (request) packets entered is enabled. Valid values are: • `yes` • `no` (default)

Table 29 NAS server attributes (continued)

Attributes	Description
`Preferred production interfaces overridden`	Indicates whether the production preferred interfaces are overridden on the replication destination.
`Preferred production IPv4 interface`	Specifies the settings for the preferred production IPv4 interface. Valid values are: • *<interface ID>* • `auto`
`Preferred production IPv6 interface`	Specifies the settings for the preferred production IPv6 interface. Valid values are: • *<interface ID>* • `auto`
`Preferred backup IPv4 interface`	Specifies the settings for the preferred backup and disaster recovery test IPv4 interface. Valid values are: • *<interface ID>* • `auto`
`Preferred backup IPv6 interface`	Specifies the settings for the preferred backup and disaster recovery test IPv6 interface. Valid values are: • *<interface ID>* • `auto`
`Source preferred production IPv4 interface`	Specifies replicated production IPv4 preferred interface settings on the replication destination. If overridden, this may be different from the `Preferred production IPv4 interface`. Valid values are: • *<interface ID>* • `auto`
`Source preferred production IPv6 interface`	Specifies replicated production IPv4 preferred interface settings on the replication destination. If overridden, this may be different from the `Preferred production IPv6 interface`. Valid values are: • *<interface ID>* • `auto`
`File space used`	Displays the total file space used for the specified NAS server.
`Data Reduction space saved`	Specifies the size saved when using data reduction for this NAS server.
`Data Reduction percent`	Specifies the storage percentage saved when using data reduction, compared to the total size used by this NAS server.
`Data Reduction ratio`	Specifies the ratio between data without data reduction, and data after data reduction savings for this NAS server.

Create a NAS server

Create a NAS server.

Note

The NFSv3 protocol is enabled by default when creating a NAS server.

Format

```
/net/nas/server create -name <value> -sp <value> {-pool <value>
| -poolName <value>} [-tenant <value>] [-mpSharingEnabled {no |
yes [-autoUserMappingEnabled {yes | no}][-unixDirectoryService
{local | ldap | nis | localThenNis | localThenLdap | none}] [-
defaultUnixUser <value>] [-defaultWindowsUser <value>]}] [-
replDest {yes [-backupOnly {yes | no}] | no}] [-
enablePacketReflect {yes | no}]
```

Action qualifiers

Qualifier	Description
`-name`	Specifies the NAS server name. **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. Value is SPA or SPB.
`-pool`	Specifies the ID of the storage pool for the NAS server.
`-poolName`	Specifies the name of the storage pool for the NAS server.
`-tenant`	Specifies the tenant identifier. **Note** If a tenant is not specified, the NAS server is created in the default network namespace.
`-mpSharingEnabled`	Indicates whether multiprotocol sharing mode is enabled. Value is yes or no (default).
`-unixDirectoryService`	Directory Service used for querying identity information for Unix (such as UIDs, GIDs, net groups). Valid values are:

Qualifier	Description
	• `nis` • `ldap` • `local` • `none` (default) • `localThenNis` • `localThenLdap`
`-autoUserMappingEnabled`	Indicates whether a Windows user who is not mapped to a known Unix/Linux username is allowed to access the NAS server's files Valid values are: • `yes`— The system generates an internal UID for the Windows user and allows access to the NAS server's files through Windows. • `no` (default)— The Windows authentication fails unless there is a default Unix username configured.
`-defaultUnixUser`	Default Unix user name or Unix ID that grants file access in the multiprotocol sharing mode. This user name or ID is used when the corresponding Unix/ Linux user name or ID is not found by the mapping mechanism. The Unix ID format is @uid=xxxx,gid=yyyy@, where xxxx and yyyy are the decimal numerical values of the UID and the primary GID, respectively. When using this ID, the user does not need to be defined in the UDS.
`-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.
`-replDest`	Replication destination settings for the NAS server. When this option is set to `yes`, only mandatory parameters may be included. All other optional parameters will be inherited from the source NAS server. Valid values are: • `yes` • `no` (default)
`-backupOnly`	Indicates whether to create NAS server as backup only. The backup only NAS server cannot be a production site, which means both planned failover and unplanned failover are disallowed in a backup only NAS server associated replication session. Valid values: • `yes` • `no`

Qualifier	Description
`-enablePacketReflect`	Indicates whether the reflection of outbound (reply) packets through the same interface that inbound (request) packets entered is enabled. Valid values are: • `yes` (default) • `no`

Example

The following command creates a NAS server with these settings:

- Name is NasServer_1.
- Associated with SP A.
- Associated with storage pool pool_0.
- IP Packet Reflect is enabled.
- The ID of the new NAS server is ID nas_1.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server
create -name NasServer_1 -sp spa -pool pool_0 -enablePacketReflect 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 (SMB) file systems or NFS file systems. You can filter on the NAS server ID.

Note

The show action command on page 23 explains how to change the output format.

Format

```
/net/nas/server [{-id <value> | -name <value> | -tenant
{<value> | none}}] show
```

Object qualifiers

Qualifier	Description
`-id`	Type the ID of a NAS server.
`-name`	Type the NAS server name.
`-tenant`	Type the tenant identifier.

Example

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

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

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

1:     ID                                        = nas_1
       Name                                      = MyVDM1
       NetBIOS name                              =
       SP                                        = spa
       Storage pool                              = pool_1
       Tenant                                    =
       Interface                                 =
       NFS enabled                               = yes
       NFSv4 enabled                             = no
       CIFS enabled                              = no
       Workgroup                                 =
       Windows domain                            =
       Multiprotocol sharing enabled             = no
       Unix directory service                    = none
       Auto user mapping enabled                 =
       Default Unix username                     =
       Default Windows username                  =
       Extended Unix credentials enabled         = no
       Credentials cache retention               = 15m
       Username translation                      =
       Packet Reflect enabled                    = yes
       Health state                              = OK (5)
       Health details                            = "The component
is operating normally. No action is required."
       Replication type                          = none
       Synchronous replication type              = none
       Replication destination                   = no
       Backup only                               = no
       Migration destination                     = no
       Preferred production interfaces overridden  =
       Preferred production IPv4 interface       = auto
       Preferred production IPv6 interface       = auto
       Preferred backup and DR test IPv4 interface = auto
       Preferred backup and DR test IPv6 interface = auto
       Source preferred production IPv4 interface  =
       Source preferred production IPv6 interface  =
       Fiel space used                           = 8945901568
(8.3G)
       Compression space saved                   = 0
       Compression percent                       = 0%
       Compression ratio                         = 1:1
       Data Reduction space saved                = 0
       Data Reduction percent                    = 0%
       Data Reduction ratio                      = 1:1
```

Change NAS server settings

Modify an existing NAS server.

Note

Manage network interfaces on page 213 explains how to modify the network interfaces associated with a NAS server.

Format

/net/nas/server {-id <*value* | -name <*value* } set [-name <*value*>] [-sp {spa | spb}] [-mpSharingEnabled {yes | no}] [-unixDirectoryService {ldap | nis | none}] [-

```
autoUserMappingEnabled {yes | no}] [{-defaultAccessDisabled |
[-defaultUnixUser <value>] [-defaultWindowsUser <value>]}] [-
enablePacketReflect {yes | no }] [-replDest {yes | no }] [-
backupOnly {yes | no}] [-preferredProductionOverride { no |
yes }][-preferredProductionIPv4 { auto | <value>}] [-
preferredProductionIPv6 { auto | <value>}] [-
preferredBackupIPv4 {auto | <value>}] [-preferredBackupIPv6
{auto | <value>}
```

Object qualifiers

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

Action qualifiers

Qualifier	Description
`-name`	Shared folder server name.
`-sp`	Owner SP. Valid values are: • spa • spb
`-mpSharingEnabled`	Indicates whether multiprotocol sharing mode is enabled. Valid values are: • `yes` • `no` **Note** You cannot disable multiprotocol file sharing for a NAS server once a file system is created on that NAS server.
`-unixDirectoryService`	Directory Service used for querying identity information for Unix (such as UIDs, GIDs, net groups). Valid values are: • `nis` • `ldap` • `local` • `none` • `localThenNis` • `localThenLdap`
`-defaultAccessDisabled`	Disables file access when no user mapping mechanism is found.
`-autoUserMappingEnabled`	Indicates whether a Windows user who is not mapped to a known Unix/Linux username is

Qualifier	Description
	allowed to access the NAS server's files Valid values are: • `yes`. The system generates an internal UID for the Windows user and allows access to the NAS server's files through Windows. • `no` (default). The Windows authentication fails unless there is a default Unix username configured.
`-defaultUnixUser`	Default Unix user name or Unix ID that grants file access in the multiprotocol sharing mode. This user name or ID is used when the corresponding Unix/Linux user name or ID is not found by the mapping mechanism. The Unix ID format is @uid=xxxx,gid=yyyy@, where xxxx and yyyy are the decimal numerical values of the UID and the primary GID, respectively. When using this ID, the user does not need to be defined in the UDS.
`-defaultWindowsUser`	Default Windows user name that grants file access in the multiprotocol sharing mode. This user name is used when the corresponding Windows user – `defaultWindowsUser` name is not found by the mapping mechanism.
`-enablePacketReflect`	Indicates whether the reflection of outbound (reply) packets through the same interface that inbound (request) packets entered is enabled. Valid values are: • `yes` • `no`
`-replDest`	Replication destination settings for the NAS server. Valid values are: • `yes` • `no`
`-backupOnly`	Indicates whether the NAS server is used as backup. Only a replication destination NAS server can be set as backup only. This attribute reflects that the NAS server cannot be the production site. This means both planned failover and unplanned failover are disallowed in the backup only NAS server associated replication session. Valid values are: • `yes`

Qualifier	Description
	• no
-preferredProductionOverride	Override the replicated production interfaces "preferred interface" settings. Valid values are: • yes • no
-preferredProductionIPv4	Production IPv4 preferred interface settings. The interface must be IPv4 and belong to this server. Valid values are: • *<interface ID>* • auto
-preferredProductionIPv6	Production IPv6 preferred interface settings. The interface must be IPv6 and belong to this server. Valid values are: • *<interface ID>* • auto
-preferredBackupIPv4	Backup and DR test IPv4 preferred interface settings. The interface must be IPv4 and belong to this server. Valid values are: • *<interface ID>* • auto
-preferredBackupIPv6	Backup and DR test IPv6 preferred interface settings. The interface must be IPv6 and belong to this server. Valid values are: • *<interface ID>* • auto

Example 1

The following command updates NAS server nas_1 with these settings:

- Enables multiprotocol sharing.
- Uses LDAP as the Unix Directory Service.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server -id nas_1 set -mpSharingEnabled yes -unixDirectoryService ldap

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

ID = nas_1
Operation completed successfully.
```

Example 2

The following command changes the replication settings for NAS server nas_1.

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

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

ID = nas_1
Operation completed successfully.
```

Example 3

The following command changes the storage processor to SPB for NAS server nas_1.

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

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

WARNING: Modifying the NAS server's SP disrupts any running NDMP
jobs, and may also result in data unavailability for some client
configurations other than NFS (v3, v4, and v4.1) and SMB3+CA. The
NDMP jobs must be restarted after the SP modification is completed.
Are you sure you want to modify the default SP?
yes / no:yes

ID = nas_1
Operation completed successfully.
```

Note

- When the SP is being modified, the NAS server health attribute is updated to INFO, and the health details attribute is updated to `Transitioning to other Storage Processor`. When the SP modification completes, the NAS server health and health details are reverted back to the previous values.
- A change to the SP cannot be performed on a NAS Server that is part of an active VDM File Import operation. The Import operation must be completed before the SP can be changed. Otherwise, the following error occurs: `Failed: Cannot complete the operation because the resource is under import. (Error Code:0x900012a).`
- A change to the SP cannot be performed on a NAS Server that is part of an active replication session. Pause the replication session, perform the SP change, and then resume the replication session. Otherwise, the following error occurs: `Cannot modify the NAS server's Storage Processor when there are non-paused replication sessions on the NAS server or its file systems. (Error Code:0x6720665).`

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.

NOTICE

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> | -name <value>} delete [{ -
cifsDomUser <value> {-cifsDomPwd <value> | -cifsDomPwdSecure} |
-skipUnjoin}]
```

Object qualifiers

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

Action qualifiers

Qualifier	Description
`-cifsDomUser`	Domain username. **Note** If the NAS server still has SMB (CIFS) servers joined to it, specify the SMB domain user to unjoin from AD before deleting the NAS server.
`-cifsDomPwd`	Domain user password. **Note** Specify the user password when you want to unjoin the CIFS server from the AD domain before deleting it.
`-cifsDomPwdSecure`	Domain user password in secure mode. This prompts the user to input the password.
`-skipUnjoin`	Does not unjoin the SMB server from the AD domain before deleting it.

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.
```

Check and update user mappings for multiprotocol NAS servers

A multiprotocol environment requires the following types of user mappings:

- A Windows user name that maps to a corresponding Unix user name
- A Unix user name that maps to a corresponding Windows user name which uses NFS to access a file system configured with a Windows access policy
- A Unix user name that is not mapped to a corresponding Windows user name which uses NFS to access a file system configured with a Unix or native access policy.

This command uses information from LDAP, NIS, or local files to parse all file systems associated with the NAS server and to update the SID/UID mapping in all nodes.

Format

```
/net/nas/server {-id <value> | -name <value>} update [-async]
{-userMapping [-dryRun] | -confView}
```

Object qualifiers

Qualifier	Description
`-id`	Type the ID of the NAS server to update.
`-name`	Type the name of the NAS server to update.

Action qualifiers

Qualifier	Description
`-async`	Perform the operation asynchronously.
`-userMapping`	For all CIFS (SMB) file systems on the NAS server, update the UID/GID and generate a user mapping report. A new UID/GID will be obtained from a Unix Directory Service for the user name of the object owner. The user name will be resolved from Active Directory by the Windows SID. **Note** Quota management and correct multiprotocol file access require correct mappings between SIDs and UIDs/GIDs at the NAS server level. Because this operation can take a significant amount of time for large file systems, it is recommended to use the `-async` qualifier.
`-dryRun`	Generate a user mapping report for downloading. Once users access a file or folder on the NAS server from the SMB protocol, their SID to UID/GID mapping is stored in an internal mapping database. This operation parses the mapping database, and for each mapped user, queries the existing Unix Directory Service and Active Directory Domain Controller to report any inconsistencies

Qualifier	Description
	between the UID/GID in the Unix Directory Service and the UID/GID stored in the database. It is recommended that you generate and review the user mapping report right before enabling multiprotocol. This enables you to ensure that your Unix Directory Service can return a UID/GID for every user whose mapping is inconsistent. Otherwise, after multiprotocol is enabled, users with inconsistent mappings may not be able to access files, because their permissions cannot be determined. Also, access to objects created by these users from SMB/CIFS cannot be granted, because the owners cannot be mapped to Unix. When the UID/GID mapping for all NAS server file systems are updated, the mapping report is re-generated automatically. **Note** Once a user successfully accesses any file or folder on the NAS server from Windows, the UID/GID in the mapping database for this user is updated. The UID/GID is also updated if the user is accessing a file from Unix for a file system with a Windows access policy.
`-confView`	Force an immediate refresh of the NAS server configuration snapshot. When the NAS server is acting as replication destination of synchronous replication session, its configuration snapshot is updated every 15 minutes by default.

Example 1

The following command generates a user mapping report for NAS server nas_1.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server -id
nas_1 update -async -userMapping
```

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

Job ID = 76
Job created successfully.
```

Example 2

The following command forces an immediate refresh of NAS server nas_1 snapshot.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server -id
nas_1 update -confView
```

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

ID = nas_1
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 30 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` (default)
`SFTP enabled`	Indicates whether the SFTP protocol is enabled. Valid values are: • `yes` • `no` (default)
`CIFS users enabled`	Indicates whether Windows (SMB) 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: • `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`

Table 30 FTP and SFTP attributes for a NAS server (continued)

Attribute	Description
`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.
`Audit enabled`	Indicates whether the FTP or SFTP server has audit file collection enabled. Valid values are: • `yes` • `no`
`Audit files directory`	Specifies the directory where the audit files for the FTP or SFTP server are stored.
`Audit file maximum size`	Specifies the maximum file size of the audit files. When the maximum is reached, a new audit file is created.
`Allowed hosts`	Specifies a comma-separated list of host IPs that are allowed access to the FTP or SFTP server. The IP can be the IPv4, IPv6, or subnet address. For subnets, the following notation convention must be used: • `10.0.0.1/10` • `2000:DB1::/10` Network names are ignored. **Note** If this option is specified, FTP/SFTP connections are allowed only for clients whose IP addresses are included in those specified in the allowed hosts list. Any clients whose IP is not specified in this list are denied access. If a subnet is defined in the allowed hosts list, the client IP must belong to the specified subnet to be allowed to connect to the NAS server. If defined, denied hosts cannot be defined.
`Allowed users`	Specifies a comma-separated list of user names that are allowed access to the FTP or SFTP server (numerical user IDs are invalid and ignored).

Table 30 FTP and SFTP attributes for a NAS server (continued)

Attribute	Description
	Note If this option is specified, FTP/SFTP connections are allowed only for the specified users. Any users not specified in this list are denied access. If defined, denied users cannot be defined.
`Allowed groups`	Specifics a comma-separated list of user groups that are allowed access to the FTP or SFTP server. Specify the name of the group (numerical group IDs are invalid and ignored). **Note** If this option is specified, FTP/SFTP connections are allowed only for the listed groups. Any user groups not specified in this list will be denied access. If defined, denied groups cannot be defined.
`Denied hosts`	Specifies a comma-separated list of host IPs that are denied access to the FTP or SFTP server. The IP can be the IPv4, IPv6, or subnet address. For subnets, the following notation convention must be used: • `10.0.0.1/10` • `2000:DB1::/10` Network names are ignored. **Note** If this option is specified, FTP/SFTP connections are denied only for clients whose IP addresses or subnet addresses are included in this list. If defined, allowed hosts cannot be defined.
`Denied users`	Specifies a comma-separated list of user names that are denied access to the FTP or SFTP server (numerical user IDs are invalid and ignored). **Note** If this option is specified, FTP/SFTP connections are denied only for the specified users. Any users not specified in this list are allowed access. If defined, allowed users cannot be defined.

Table 30 FTP and SFTP attributes for a NAS server (continued)

Attribute	Description
`Denied groups`	Specifics a comma-separated list of user groups that are denied access to the FTP or SFTP server. Specify the name of the group (numerical group IDs are invalid and ignored). **Note** If this option is specified, FTP/SFTP connections are denied only for the listed groups. Any user groups not specified in this list will be allowed access. If defined, allowed groups cannot be defined.

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 associated 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: 10.0.0.1
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
        Allowed hosts             =
1.2.3.10,1.2.3.11,192.168.0.0/16,2001:db8::/48
        Allowed users             =
        Allowed groups            =
        Denied hosts              =
        Denied users              = guest,jack,john
        Denied groups             = guests,group1
```

Change FTP settings

Modify existing FTP or SFTP settings of a NAS server.

Format

```
/net/nas/ftp -server <value> set [-ftpEnabled <value>] [-
sftpEnabled <value>] [-cifsUserEnabled <value>] [-
unixUserEnabled <value>] [-anonymousUserEnabled <value>] [-
homedirLimitEnabled <value>] [-defaultHomedir <value>] [-
welcome <value>] [-motd <value>] [-auditEnabled {yes|no}] [-
auditDir <value>] [-auditMaxSize <value>] {[-allowHost <value>]
| [-appendAllowHost <value>] | [-removeAllowHost <value>] | [-
denyHost <value>] | [-appendDenyHost <value>] | [-
removeDenyHost <value>]} {[-allowUser <value>] | [-
appendAllowUser <value>] | [-removeAllowUser <value>] | [-
denyUser <value>] | [-appendDenyUser <value>] | [-
removeDenyUser <value>]} {[-allowGroup <value>]| [-
appendAllowGroup <value>] | [-removeAllowGroup <value>] |[-
denyGroup <value>] | [-appendDenyGroup <value>] | [-
removeDenyGroup <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`
`-sftpEnabled`	Indicates whether the SFTP server is enabled on the NAS server. Valid values are: • `yes` • `no`
`-cifsUserEnabled`	Indicates whether Windows (SMB) users can be authenticated by the FTP or SFTP server. Valid values are: • `yes` • `no`
`-unixUserEnabled`	Indicates whether Unix users can be authenticated by the FTP or SFTP server. Valid values are: • `yes` • `no`
`-anonymousUserEnabled`	Indicates whether the FTP server supports anonymous user authentication. Valid values are: • `yes` • `no`

Qualifier	Description
-homedirLimitEnabled	Indicates whether authenticated FTP or SFTP users are limited to their home directories. Valid values are: - yes - 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.
-motd	Type the message of the day that appears once the FTP or SFTP users log on.
-auditEnabled	Indicates whether FTP/SFTP auditing is enabled on the NAS server. Valid values are: - yes - no
-auditDir	Type the directory where the audit files should be saved.
-auditMaxSize	Type the maximum size for the audit log file. When this maximum is exceeded, a new audit file is created.
-allowHost	Type the comma-separated list of allowed client host IPs. The IP can be the IPv4, IPv6, or subnet address. For subnets, the following notation convention must be used: - 10.0.0.1/10 - 2000:DB1::/10 Network names are ignored. **Note** If specified, FTP/SFTP connections are allowed only for clients whose IP addresses are included in those specified in the allowed hosts list. Any clients whose IP is not specified in this list are denied access. If a subnet is defined in the allowed hosts list, the client IP must belong to the specified subnet to be allowed to connect to the NAS FTP/SFTP server. If –allowHost is defined, -denyHost cannot be defined.
-appendAllowHost	Specify one or multiple comma-separated host IPs to append to existing list of allowed host IP addresses.
-removeAllowHost	Specify one or multiple comma-separated host IPs to remove from the existing list of allowed host IP addresses.

Qualifier	Description
`-denyHost`	Type the comma-separated list of client host IPs that will be denied access to the FTP/SFTP server. The IP can be the IPv4, IPv6, or subnet address. For subnets, the following notation convention must be used: • `10.0.0.1/10` • `2000:DB1::/10` Network names are ignored. **Note** If specified, FTP/SFTP connections are denied only for clients whose IP addresses are included in those specified in the `-denyHost` list. Any clients whose IP is not specified in this list are allowed access. If a subnet is defined in the denied hosts list, client IPs which belong to the specified subnet will be denied access to the NAS FTP/SFTP server. If `-denyHost` is defined, `-allowHost` cannot be defined.
`-appendDenyHost`	Specify one or multiple comma-separated host IPs to append to existing list of denied host IP addresses.
`-removeDenyHost`	Specify one or multiple comma-separated host IPs to remove from the existing list of denied host IP addresses.
`-allowUser`	Type the comma-separated list of user names that will be allowed access to the FTP/SFTP server (numerical user IDs are invalid and ignored). **Note** If this option is specified, FTP/SFTP connections are allowed only for the specified users. Any users not specified in this list are denied access. If `-allowUser` is defined, `-denyUser` cannot be defined.
`-appendAllowUser`	Specify one or multiple comma-separated user names to append to existing list of allowed users.
`-removeAllowUser`	Specify one or multiple comma-separated user names to remove from the existing list of allowed users.
`-denyUser`	Type the comma-separated list of user names that will be denied access to the FTP/SFTP server (numerical user IDs are invalid and ignored).

Qualifier	Description
	Note If this option is specified, FTP/SFTP connections are denied only for the specified users. Any users not specified in this list are denied access. If `-denyUser` is defined, `-allowUser` cannot be defined.
`-appendDenyUser`	Specify one or multiple comma-separated user names to append to existing list of denied users.
`-removeDenyUser`	Specify one or multiple comma-separated user names to remove from the existing list of denied users.
`-allowGroup`	Type the comma-separated list of user group names that will be allowed access to the FTP/SFTP server (numerical group IDs are invalid and ignored). **Note** If this option is specified, FTP/SFTP connections are allowed only for the listed groups. Any user groups not specified in this list will be denied access. If –`allowGroup` is defined, –`denyGroup` cannot be defined.
`-appendAllowGroup`	Specify one or multiple comma-separated user group names to append to existing list of allowed groups.
`-removeAllowGroup`	Specify one or multiple comma-separated user group names to remove from the existing list of allowed groups.
`-denyGroup`	Type the comma-separated list of user group names that will be denied access to the FTP/SFTP server (numerical group IDs are invalid and ignored). **Note** If this option is specified, FTP/SFTP connections are denied only for the listed groups. Any user groups not specified in this list will be allowed access. If –`denyGroup` is defined, –`allowGroup` cannot be defined.
`-appendDenyGroup`	Specify one or multiple comma-separated user group names to append to existing list of denied groups.
`-removeDenyGroup`	Specify one or multiple comma-separated user group names to remove from the existing list of denied groups.

Example 1

```
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.
```

Example 2

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/ftp -server
nas_1 set -denyUser "guest,jack,john" -appendAllowHost 1.2.3.4,1.2.3.5
```

```
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 (IDMU), IPLANET schema, or an RFC 2307 (open LDAP) schema. By default, the RFC 2307 schema is generated. Once the schema is identified, it 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 31 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.
`Servers`	Relevant IP addresses of the associated LDAP servers. If you want the NAS server to use DNS service discovery to obtain LDAP server IP addresses automatically, do not specify a value for this option. **Note** For the automatic discovery process to work, the DNS server must contain pointers to the LDAP servers, and the LDAP servers must share the same authentication settings.

Table 31 LDAP settings of a NAS server (continued)

Attribute	Description
`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 `636`.
`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`
`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 to authenticate to the LDAP server. Valid values are: - `yes` – Indicates that the CIFS (SMB) settings are used for Kerberos authentication. This option is commonly used when configuring IDMU as a Unix directory service. - `no` – Indicates that Kerberos uses its own settings. See Configure Kerberos settings on page 164 to configure authentication through the Kerberos realm.
`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.

Table 31 LDAP settings of a NAS server (continued)

Attribute	Description
`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 in RFC notation, or specifies the dotted domain name.
`Profile DN`	For an iPlanet LDAP server, specifies the DN of the entry with the configuration profile.
`Replication sync`	Indicates the status of the LDAP servers addresses list in the NAS server operating as a replication destination. When a replicated LDAP servers list is created on the source NAS server, it is automatically synchronized to the destination. Valid values are: • `Not replicated` – LDAP list is not replicated over to the destination. • `Auto synchronized` – LDAP list is automatically synchronized over to the replication destination. Any modify or delete operations at the source will automatically be reflected on the destination. • `Overridden` – LDAP list has been manually modified or overridden on the replication destination. Modifications or deletions of addresses from the LDAP list on the source NAS server will have no effect on the overridden DNS list on the replication destination. **Note** When a LDAP list is disabled or deleted from the source, overridden LDAP list in the destination may not get disabled or deleted automatically.
`Source servers`	List of LDAP server IP addresses defined on the replication source.

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
```

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

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=emc,dc=com
   Profile DN         =
   Replication sync = Not replicated
   Source servers     =
```

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>]} [-replSync {auto | overridden}]
```

Object qualifier

Qualifier	Description
`-server`	Identifies the associated NAS server.

Action qualifier

Qualifier	Description
`-enabled`	Specify to disable LDAP for an existing NAS server. Valid value is `no`. **Note** Setting the value to no removes the LDAP settings for an existing NAS server.

Qualifier	Description
`-ip`	Type the IP addresses (separated by comma) of the associated LDAP servers. If you want the NAS server to use DNS service discovery to obtain LDAP server IP addresses automatically, do not specify a value for this option. **Note** For the automatic discovery process to work, the DNS server must contain pointers to the LDAP servers, and the LDAP servers must share the same authentication settings.
`-port`	Type the port associated with the LDAP server. If LDAPS is used, the default is 363. If LDAP is used, the default port is 389.
`-protocol`	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` 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` (valid only when `simple` authentication is used)	Type the Distinguished Name (DN) to be used when binding to the server.
`-bindPasswd` (valid only when `simple` authentication is used)	Type the associated password to be used when binding to the server.
`-bindPasswdSecure` (valid only when `simple` authentication is used)	Type the password in secured mode. You will be prompted to enter the password separately.
`-useCifsAccount` (valid only when `kerberos` authentication is used)	Specify whether you want to use CIFS (SMB) authentication. For Kerberos authentication only. Commonly used to configure NAS servers to use IDMU as a Unix Directory Service. (Choose `simple` authentication to authenticate AD without using a CIFS account.)

Qualifier	Description
`-principal` (valid only when `kerberos` authentication is used)	Type the principal name for Kerberos authentication.
`-realm` (valid only when `kerberos` authentication is used)	Type the realm name for Kerberos authentication.
`-password` (valid only when `kerberos` authentication is used)	Type the associated password for Kerberos authentication.
`-baseDn`	Type the DN of the root level in the directory tree in RFC notation, or type the dotted domain name. Valid notation formats include: • RFC, for example <*dc=nt2k80, dc=drm,dc=lab,dc=emc,dc=com*> • Dotted domain name, for example <*nt2k80.drm.lab.emc.com*>
`-profileDn`	For an iPlanet LDAP server, type the DN of the entry with the configuration profile.
`-replSync`	Status of the LDAP addresses servers list in the NAS server operating as a replication destination. Valid values are: • `auto` • `overridden`

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 -protocol ldaps
-authType simple -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 an `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 20.

Example

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! -download /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 -d 10.0.0.1 -u Local/joe -p MyPassword456! –download /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 NAS interfaces

NAS interfaces represent the network interface configured on an Ethernet port for a NAS server.

Table 32 Interface attributes

Attribute	Description
`ID`	ID of 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` • `no` **Note** This attribute applies to file interfaces only.
`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. For IP multi-tenancy, the VLAN ID of a NAS server interface must comply with the set of VLAN IDs assigned to a tenant to which the NAS server belongs. Only unassigned VLAN IDs are allowed for NAS servers that do not belong to a tenant. **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.
`Role`	Specifies the use of the file interface. Valid values are: • `production` • `backup` Backup interfaces are only available for backup via NFS and NDMP protocols, and are not available for CIFS (SMB) protocol. Interfaces associated with NAS servers in a replication session are not replicated via the replication session. You can create a backup interface on the destination NAS server. Unlike production interfaces, backup interfaces become instantly active on the

Table 32 Interface attributes (continued)

Attribute	Description
	destination NAS server and enable you to perform backup and disaster recovery testing via the NFS share over the snapshot.
Replication sync	Applies to production interfaces replicated over replication sessions. Valid values are: • Not replicated • Auto synchronized – indicates that such interface is automatically synchronized over the replication session to the destination. Any modify and delete operations on the source will be automatically reflected on the destination. • Overridden – indicates that such interface is manually modified / overridden on the destination side. When a replication production interface is created on the source NAS server, it is auto-synchronized to the destination. **Note** Modifications or deletions of network settings of the corresponding source IP interfaces have no effect on overridden interface on destination. However, when an interface is deleted on the source, overridden interfaces stop responding and health state values of such interfaces become degraded/warning. This is because the SMB/CIFS shares are tightly set to the production IP interfaces, and they will not operate via overridden interfaces after a failover.
Health state	A numerical value indicating the health of the system. Valid values are: • Unknown (0) • OK (5) • OK BUT (7) • Degraded/Warning (10) • Minor failure (15) • Major failure (20)
Health details	Additional health information.
Source VLAN ID	Indicates the value of the corresponding VLAN ID as defined on the source NAS server in a replication session.
Source IP address	Indicates the value of the corresponding IP address as defined on the source NAS server in a replication session.
Source subnet mask	Indicates the value of the corresponding subnet mask as defined on the source NAS server in a replication session.
Source gateway	Indicates the value of the corresponding gateway as defined on the source NAS server in a replication session.

Create a NAS interface

Create a NAS interface.

Format

```
/net/nas/if create [-vlanId <value>] {-server <value> | -
serverName <value>} [-preferred] -port <value> -addr <value>]
[-netmask <value>] [-gateway <value>] [-role {production |
backup}]
```

Action qualifiers

Qualifier	Description
`-server`	NAS server identifier. **Note** A NAS server cannot have more than one IPv4 interface and one IPv6 interface.
`-serverName`	NAS server name. **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. That means that all outgoing DNS or Active Directory requests will be forwarded though interface marked as preferred and will use the IP address assigned to this interface as a source address of the packets. **Note** 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. **Note** On dual SP systems, a file interface is created on a pair of symmetric Ethernet ports (or link aggregations) 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 spa_eth2, but the NAS server current SP is SP B, the interface is created on spb_eth2 instead).
`-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.

Qualifier	Description
	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.
`-role`	Specify the role of the interface. Valid values are: • `production` (default) • `backup` **Note** To create an interface on a NAS server operating as a replication destination, specify the value as `backup`.

Example

The following command creates a NAS interface. The interface receives the ID IF_2:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/if create -
server nas_1 -port eth0_SPA -addr 10.0.0.1 -netmask 255.255.255.0
```

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

ID = IF_2
Operation completed successfully.
```

View NAS interfaces

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

Note

The show action command on page 23 explains how to change the output format.

Format

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

Object qualifiers

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.
-serverName	Type the name of the NAS server the interface is associated with.

Example

The following command displays all NAS interfaces on the system:

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

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

1:     ID                      = if_0
       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
       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 NAS interface settings

Change the settings for a NAS interface.

Format

```
/net/nas/if -id <value> set [-vlanId <value>] [-addr <value>]
[-netmask <value>] [-gateway <value>][-preferred] [-replSync
{auto | overridden}]
```

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.
`-replSync`	Applicable only to NAS server acting as replication destination. Any modification to network address information automatically switches the interface into overridden mode. Valid values are: • auto • overridden Note the following:

Qualifier	Description
	• Use this qualifier to switch an interface back into "auto" synchronization and clear all overridden settings. • When the corresponding interface is already deleted on the source, when replication sync is set to "auto", it will also cause deletion of the interface on destination. • Value "overridden" will cause network interfaces to stop being automatically synchronized. Current settings on the source system will become "frozen" and auto-propagation will stop.

Example

The following command changes the gateway address for interface IF_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456!/net/nas/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 NAS interfaces

Delete a NAS interface.

⚠ CAUTION

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

Format

```
/net/nas/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/nas/if -id IF_1
delete
```

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

Operation completed successfully.
```

Manage NAS routes

A NAS route represents a route configured on a NAS interface.

Table 33 NAS route attributes

Attribute	Description
`ID`	ID of the route.
`NAS server`	NAS server identifier.
`Interface`	ID of the interface used to reach the gateway.
`Route type`	Type of route. Valid values are (case-insensitive): • `default` – The system uses a default gateway/route when it cannot find a more specific host or network route to a given destination. One default IPv4 and IPv6 route is allowed per interface. • `host` – Creates a route to a host. • `net` – Creates a route to a subnet.
`Target`	IP address for the target network node based on the value of `-type`. Value is one of the following: • For a default route, the system will use the IP address specified for `-gateway`. • For a host route, specify the IP address of a target host. • For a net route, specify the IP address of a target subnet. Include the `-netmask` qualifier for the target subnet.
`Netmask`	Subnet mask.
`Gateway`	Gateway address.
`Replication sync`	If the route source is a NAS server production interface, this is a copy of the `Replication sync` attribute of the associated interface. (The associated interface is specified in the `Interface` attribute). If the route source is not a NAS server production interface, the value of this attribute is empty.
`Health state`	Numerical value indicating the health of the system. Valid values are: • `Unknown (0)` • `OK (5)` • `OK BUT (7)` • `Degraded/Warning (10)` • `Minor failure (15)` • `Major failure (20)`
`Health details`	Additional health information.
`Use for external services access`	Flag indicating whether the route is used for access to external services. Valid values are: • `yes` • `no`

Create a NAS route

Create a route for a NAS interface.

Format

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

Action qualifiers

Qualifier	Description
`-if`	Specify the interface associated with the route. Each interface has its own routing table for use in responding to inbound service requests.
`-type`	Specify the type of route. Valid values are (case-insensitive): • `default` – System uses the default route/gateway when a more specific host or network route is not available. One default IPv4 and IPv6 route is allowed per interface. • `host` – Create a route to a host. • `net` – Create a route to a subnet.
`-target`	Specify the IP address for the target network node based on the value of `-type`: • For a default route, do not specify a value. • For a host route, specify the IP address of a target host. • For a net route, specify the IP address of a target subnet. Include the `-netmask` qualifier for the target subnet.
`-netmask`	For a route to a subnet, specify the netmask of the destination subnet.
`-gateway`	Specify the gateway for the route.

Example

The following command creates a network route for interface if_1 to reach the 10.64.74.x subnet using gateway 10.64.74.1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/route
create -if if_1 -type net -target 10.64.200.10 -netmask 255.255.255.0
-gateway 10.64.74.1
```

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

ID = route_1
Operation completed successfully.
```

Change NAS route settings

Change the settings for a NAS route.

Format

```
/net/nas/route -id <value> set [-type {default | host | net}]
[-target <value>] [-netmask <value>] [-gateway <value>]
```

Object qualifier

Qualifier	Description
`-id`	Identifies the NAS route object.

Action qualifiers

Qualifier	Description
`-type`	Specify the type of route. Valid values are (case-insensitive): • `default` – System uses the default route/gateway when a more specific host or network route is not available. One default IPv4 and IPv6 route is allowed per interface. • `host` – Create a route to a host. • `net` – Create a route to a subnet.
`-target`	Specify the IP address for the target network node based on the value of `-type`. Valid values are: • For a default route, do not specify a value. The system will use the IP address specified for `-gateway`. • For a host route, specify the IP address of a target host. • For a net route, specify the IP address of a target subnet. Include the `-netmask` qualifier for the target subnet.
`-netmask`	For a route to a subnet, specify the netmask of the destination subnet.
`-gateway`	Specify the gateway for the route.

Example

The following command changes the target IP address to 10.64.200.11, the netmask to 255.255.255.0, and the gateway to 10.64.74.2 for NAS route route_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456!/net/nas/route -id
route_1 set -target 10.64.200.11 -netmask 255.255.255.0 -gateway
10.64.74.2 uemcli
```

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

ID = route_1
Operation completed successfully.
```

View NAS routes

View a list of routes for a specified NAS interface or for all NAS interfaces on the system.

Note

The show action command on page 23 explains how to change the output format.

Format

/net/nas/route [{-id *<value>* | -server *<value>* [-useForESAccess {yes | no}] | -if *<value>*}] show

Object qualifiers

Qualifier	Description
-id	Specify the ID of the route.
-server	Specify the NAS server for which to view routes.
-useForESAccess	Indicate whether you want the system to display only the routes that are used for external services.
-if	Indicate whether you want the system to display only the routes associated with the specified NAS server.

Example

The following command displays all NAS routes on the system:

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

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

1:    ID                             = route_1
      NAS server                     = nas_1
      Type                           = net
      Target                         = 10.50.50.10
      Netmask                        = 255.255.255.0
      Gateway                        = 10.0.0.1
      Interface                      = if_1
      Health state                   = OK (5)
      Health details                 = "The component is
operating normally. action is required."
      Replication sync               =
      Use for external services access = no


2:    ID                             = route_2
      NAS server                     = nas_1
      Type                           = default
      Target                         =
      Netmask                        =
      Gateway                        = 10.0.0.2
      Interface                      = if_2
      Health state                   = OK (5)
      Health details                 = "The component is
operating normally. No action is required."
      Replication sync               =
      Use for external services access = no

3:    ID                             = route_3
      NAS server                     = nas_1
      Type                           = host
      Target                         = 10.50.50.168
      Netmask                        =
      Gateway                        = 10.0.0.3
      Interface                      = if_3
      Health state                   = OK (5)
      Health details                 = "The component is
operating normally. No action is required."
```

```
      Replication sync                 =
      Use for external services access = yes
```

Delete NAS routes

Delete a NAS route.

⚠ CAUTION

Deleting a NAS route can break the connection between systems that use it, such as configured hosts.

Format

/net/nas/route -id *<value>* delete

Object qualifier

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

Example

The following command deletes route route_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/route -id
route_1 delete
```

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

Operation completed successfully.
```

Manage Kerberos settings

Settings for custom Kerberos key distribution center servers.

Kerberos is a distributed authentication service designed to provide strong authentication with secret-key cryptography. It works on the basis of "tickets" that allow nodes communicating over a non-secure network to prove their identity in a secure manner. When configured to act as a secure NFS server, the NAS server uses the RPCSEC_GSS security framework and Kerberos authentication protocol to verify users and services. You can configure a secure NFS environment for a multiprotocol NAS server or one that supports Unix-only shares. In this environment, user access to NFS file systems is granted based on Kerberos principal names.

Table 34 Kerberos attributes

Attribute	Description
NAS server	Kerberos realm configuration object, as identified by the NAS server ID.
Realm	Name of the Kerberos realm.

Table 34 Kerberos attributes (continued)

Attribute	Description
`Servers`	Comma separated list of DNS names for the Kerberos Key Distribution Center (KDC) servers.
`Port`	KDC servers TCP port. Default: 88.

Configure Kerberos settings

Set Kerberos settings for a NAS server.

Format

```
/net/nas/kerberos -server <value> set {-enabled no | [ -addr
<value>] [-port <value>] [-realm <value>]}
```

Object qualifier

Qualifier	Description
`-server`	Identifies the associated NAS server.

Action qualifiers

Qualifier	Description
`-enabled`	Enables Kerberos on the NAS server. Value is `yes` or `no`.
`-addr`	Specifies the DNS names of the Kerberos KDC servers, separated by commas. **Note** Setting addresses via IP and overriding them is not supported in this release. A fully qualified DNS name is expected.
`-port`	Specifies the TCP port of the KDC server. Value is any TCP port.
`-realm`	Identifies the Kerberos realm. When non-unique for the system, the operation returns an error.

Example

The following command configures a custom Kerberos realm for NAS server nas_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/kerberos -
server nas_1 set -addr
"master.mydomain.lab.emc.com,slave.mydomain.emc.com" -realm
"MYDOMAIN.LAB.EMC.COM"
```

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

Operation completed successfully.
```

View Kerberos settings

View Kerberos settings.

Format

```
/net/nas/kerberos [{-server <value> | -realm <value>}] show
```

Object qualifiers

Qualifier	Description
-server	Identifies the associated NAS server.
-realm	Identifies the associated Kerberos realm.

Example

The following command shows Kerberos settings for all of the storage system's NAS servers.

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

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

1:    NAS server = nas_2
      Realm      = TEST.LAB.EMC.COM
      Servers    = us67890.test.lab.emc.com

2:    NAS server = nas_1
      Realm      = TEST.LAB.EMC.COM
      Servers    = us12345.test.lab.emc.com
```

Manage VLANs

Network partitioning is provided through Virtual LANs. VLANs are statically allocated in the system, and the only allowed actions are to assign or de-assign a VLAN ID either to or from a specific tenant.

Each VLAN is identified by an ID.

The following table lists the attributes for VLANs.

Table 35 VLAN attributes

Attribute	Description
ID	VLAN identifier.
Tenant	Tenant identifier, if assigned.
Interface	List of network interfaces that use this VLAN ID for network traffic tagging.

View VLANs

View details about configured VLANs. You can filter on the ID of the VLAN.

Format

```
/net/vlan show {-id <value> | [-from <value>] [-count <value>]
[-inUse {yes | no}] [-assigned {yes [-tenant <value>] | no}]}
```

Action qualifiers

Qualifier	Description
`-id`	Identifies the VLAN ID. Valid values are 1 to 4095. If specified, no other VLAN ID range, network interface or tenant assignment selectors are allowed.
`-from`	Specifies the lower boundary of the VLAN range to be displayed. Valid values are 1 to 4095. If omitted, the default value is 1.
`-count`	Specifies the number of items to be displayed. Valid values are 1 to 4095. If omitted, the default value is 10.
`-inUse`	Valid values are: • `yes` — Shows only those VLANs being used by a network interface. These VLANs cannot be moved to or from another tenant. • `no` — Shows only those VLANs that are not being used by a network interface.
`-assigned`	Valid values are: • `yes` — Shows only those VLANs that are assigned to a tenant. • `no` — Shows only those VLANs that are not assigned to a tenant.
`-tenant`	If specified, identifies the tenant.

Example

The following command displays information for VLANs that are in use starting from 100:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/vlan show -from
100 -inUse yes
```

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

1:      VLAN      = 101
        Tenant    = tenant_1
        Interface = if_1,if_3

2:      VLAN      = 105
        Tenant    =
        Interface = if_5
```

Manage tenants

IP multi-tenancy provides the ability to assign multiple network namespaces to the NAS Servers on a storage processor. Tenants are used to create isolated file-based (CIFS/NFS) storage partitions. This enables cost-effective tenant management of available resources while ensuring that tenant visibility and management are restricted to assigned resources only.

Each tenant can have its own:

- VLAN domain
- Routing table
- IP firewall
- Virtual interface, traffic separated from virtual device and in Linux Kernel layer
- DNS server or other administrative servers to allow the tenant to have its own authentication and security validation from the Protocol layer

Each tenant is identified by a Universally Unique Identifier (UUID).

The following table lists the attributes for tenants.

Table 36 Tenant attributes

Attribute	Description
`ID`	Tenant identifier
`Name`	Friendly name of the tenant.
`UUID`	Universally unique identifier of a tenant.
`VLAN`	Comma-separated list of VLAN IDs assigned to the tenant.

Create a tenant

Create a tenant.

Format

```
/net/tenant create -name <value> -uuid <value> [-vlan <value>]
```

Action qualifiers

Qualifier	Description
`-name`	Specify the tenant name.
`-uuid`	Specify the Universally Unique Identifier of a tenant.
`-vlan`	Specify the comma-separated list of VLAN IDs that the tenant can use. **Note** Valid values are 1 to 4095; however, each specific VLAN ID can be assigned to a tenant if: 1. It is not assigned to any other tenant. 2. No existing network interfaces are tagged with the VLAN ID.

Example

The following command creates a tenant with these settings:

- Tenant name is Tenant A.
- UUID is b67cedd7-2369-40c5-afc9-9e8753b88dee.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/tenant create -
name "Tenant A" -uuid b67cedd7-2369-40c5-afc9-9e8753b88dee
```

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

ID = tenant_1
Operation completed successfully.
```

View tenants

View details about configured tenants. You can filter on the ID of the tenant.

Format

```
/net/tenant [-id <value>] show
```

Object qualifier

Qualifier	Description
-id	Identifies the tenant to be displayed.

Example

The following command displays tenant information:

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

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

1:     ID     = tenant_1
       Name   = Tenant A
       UUID   = b67cedd7-2369-40c5-afc9-9e8753b88dee
       VLAN   = 102,103,104
```

Change tenant settings

Change the settings for a tenant.

Format

```
/net/tenant –id <value> set [ -name <value> ] { [-vlan <value>]
| [-addVlan <value>] | [-removeVlan <value>] }
```

Object qualifier

Qualifier	Description
-id	Identifies the tenant.

Action qualifiers

Qualifier	Description
-name	Specify the new name of the tenant.
-vlan	Specify the comma-separated list of VLAN IDs.

Qualifier	Description

	Note
	Valid values for VLAN IDs are 1 to 4095. The new set of VLAN IDs is compared against VLAN IDs already assigned to this tenant. Mismatches are interpreted as if respective IDs were passed to `–addVlan` or `–removeVlan` qualifiers. For example, if VLANs 101,102, and103 are assigned to tenant X, the command:
	`tenant -id X set -Vlan 101,102,104`
	is equivalent to:
	`tenant -id X set -removeVlan 103`
	`tenant -id X set -addVlan 104`

`-addVlan`	Specify the VLAN ID to be assigned to the tenant. **Note** Valid values for VLAN IDs are 1 to 4095; however, each specific VLAN ID can be assigned to a tenant if: 1. It is not assigned to any other tenant. 2. No existing network interfaces are tagged with the VLAN ID.
`-removeVlan`	Specify the VLAN ID to be removed from the tenant. **Note** The VLAN ID can be removed only if it is not in use by any interface of any NAS server within this tenant.

Example

The following command changes the tenant settings for the list of VLAN IDs:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/tenant -id
tenant_1 set -vlan 101,102,104
```

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

Operation completed successfully.
```

Delete a tenant

Deletes an existing tenant. When you delete an existing tenant, the VLANs associated with that tenant become available for use with other tenants.

Format

```
/net/tenant -id <value> delete
```

Object qualifiers

Qualifier	Description
`-id`	Identifies the tenant.

Example

The following command deletes a tenant.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/tenant -id
tenant_1 delete
```

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

ID = tenant_1
Operation completed successfully.
```

Manage CIFS Servers

CIFS (SMB) 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 stand-alone CIFS server.

The following table lists the attributes for CIFS servers.

Table 37 CIFS Server attributes

Attribute	Description
`ID`	ID of the CIFS server.
`NAS server`	Associated NAS server ID.
`Name`	Name of the CIFS server account used when joining the Active Directory.
`Description`	Description 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.
`Last used organization unit`	Last used Active Directory organizational unit.
`Workgroup`	Workgroup name.
`Workgroup administrator password`	Workgroup administrator password.

Create a CIFS server

Create a CIFS (SMB) server.

Note

Only one CIFS server per NAS server can be created.

Format

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

Action qualifiers

Qualifier	Description
`-server`	Specifies the NAS server identifier.
`-serverName`	Specifies the NAS server name.
`-name`	Specifies the CIFS server name. By default, this is the same as the value for `serverName`. This value is ignored if the CIFS server is standalone.
`-description`	Specifies the description of the CIFS server.
`-netbiosName`	Specifies the CIFS server NetBIOS name. By default it is generated automatically based on the CIFS server name.
`-domain` (valid only when joining the CIFS server to AD)	Specifies Windows Active Directory domain name.
`-username` (valid only when joining the CIFS server to AD)	Specifies the Active Directory user that will be used to join the CIFS server to AD.
`-passwd` (valid only when joining the CIFS server to AD)	Specifies the AD user password.
`-passwdSecure` (valid only when joining the CIFS server to AD)	Specifies the password in secure mode. The user will be prompted to input the password and the password confirmation.
`-orgUnit` (valid only when joining the CIFS server to AD)	Active directory organizational unit.
`-workgroup` (valid only when configuring a stand-alone CIFS server)	Specifies the workgroup of the stand-alone `-workgroup` CIFS server.
`-adminPasswd` (valid only when configuring a stand-alone CIFS server)	Specifies the local administrator account password of the stand-alone CIFS server.
`-adminPasswdSecure` (valid only when configuring a stand-alone CIFS server)	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 nas_0 -name CIFSserver1 -description "CIFS description" -
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 (SMB) server settings.

Format

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

Object qualifiers

Qualifier	Description
`-id`	Type the ID of the CIFS server.
`-name`	Type the name of the CIFS server.
`-server`	Type the ID of the associated NAS server.
`-serverName`	Type the name of 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
       NAS server     = nas_0
       Name           = CIFSserver1
       Description    = CIFS description
       NetBIOS name   = CIFSserv
       Windows domain = domain.one.com
```

Change CIFS server settings

Modify an existing CIFS (SMB) server.

If moving a CIFS server from one domain to another, include the following options:

- `[-domain <value>]`
- `[-newUsername <value> {-newPasswd <value> | -newPasswdSecure}]`

Note that you must specify the username and password of the domain to which the CIFS server was previously joined in order to perform the unjoin. You must also specify the user name and password of the new domain to which it will be joined.

Format

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

Object qualifiers

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

Action qualifiers

Qualifier	Description
-name	Specifies the new CIFS server name.
-description	Specifies the description of the CIFS server.
-netbiosName	Specifies the new CIFS server NetBIOS name.
-domain	Specifies the new Windows server domain name.
-orgUnit	Active Directory organizational unit.
-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.
-skipUnjoin	Do not unjoin the CIFS server from an AD domain.
-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 stand-alone CIFS server.
-adminPasswd	Specifies the new local admin password of the stand-alone 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 a CIFS server

Delete an existing CIFS (SMB) server.

Note

When you delete an existing CIFS server or convert it to a stand-alone configuration, you must specify the current credentials (username and password) to properly unjoin it from the domain and remove the computer account from Active Directory. You can use the `-skipUnjoin` option to delete the CIFS server without removing the computer account from AD. (This will require the administrator to manually remove the account from AD.) The `-skipUnjoin` option can also be used when AD is not operational or cannot be reached. 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> | -name <value>} delete [ {-username
<value> {-passwd <value> | -passwdSecure} | -skipUnjoin} ]
```

Object qualifiers

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

Action qualifiers

Qualifier	Description
`-username`	Specifies the domain username. Not required for stand-alone CIFS servers. **Note** Specify the username when you want to unjoin the CIFS server from the AD domain before deleting it.
`-passwd`	Specifies the domain user password. Not required for stand-alone CIFS servers.

Qualifier	Description
	Note Specify the user password when you want to unjoin the CIFS server from the AD domain before deleting it.
`-passwdSecure`	Specifies the password in secure mode. This prompts the user to input the password.
`-skipUnjoin`	Does not unjoin the CIFS server from the AD domain before deleting it.

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 NFS servers

NFS servers use the NFS protocol to transfer files.

The following table lists the attributes for NAS servers.

Table 38 NFS Server attributes

Attribute	Description
`ID`	ID of the NFS server.
`NAS server`	Associated NAS server ID.
`Hostname`	NFS server hostname. When an SMB server is joined to an Active Directory (AD) domain, the NFS server hostname is defaulted to the SMB computer name. If you configure NFS secure to use a custom realm for Kerberos authentication, this hostname can be customized.
`NFSv3 enabled`	Indicates whether NFS shares can be accessed by using the NFSv3 protocol. Valid values are `yes` or `no` (default is `yes`).
`NFSv4 enabled`	Indicates whether NFS shares can be accessed by using the NFSv4 protocol. Valid values are `yes` or `no` (default is `no`).
`Secure NFS enabled`	Indicates whether secure NFS (with Kerberos) is enabled. Value is yes or no.

Table 38 NFS Server attributes (continued)

Attribute	Description
`Kerberos KDC type`	Indicates the type of KDC realm to use for NFS secure. Value is one of the following: • `Windows` — Use the Windows realm associated with the SMB server configured on the NAS server. If you configure secure NFS using this method, SMB support cannot be deleted from the NAS server while secure NFS is enabled and configured to use the Windows realm. • `custom` — Configure a custom realm to point to any type of Kerberos realm. (Windows, MIT, Heidmal). If you configure secure NFS using this method, you must upload the keytab file to the NAS server being defined. Refer to Configure Kerberos settings on page 164 for more information.
`Service principal name`	Comma-separated list of service principal names to used to authenticate to the Kerberos realm. The name is automatically deducted from the NFS server hostname and the selected realm.
`Extended Unix credentials enabled`	Use more than 16 Unix groups. Value is yes or no (default).
`Credentials cache retention`	Credentials cache refreshing timeout, in minutes.

Create an NFS server

Create an NFS server.

Note

Only one NFS server per NAS server can be created.

Format

```
/net/nas/nfs create {-server <value> | -serverName <value>} [-
hostname <value>] [-v3 {yes | no}][-v4 {yes | no}] [-secure {no
| yes [-kdcType {Windows | custom}]}] [-username <value> {-
passwd <value> | -passwdSecure}] [-extendedUnixCredEnabled
{yes|no}] [-credCacheRetention <value>]
```

Action qualifiers

Qualifier	Description
`-server`	Specifies the NAS server identifier.
`-serverName`	Specifies the NAS server name.

Qualifier	Description
`-hostname`	Specifies the hostname for the NFS server. This is used in Kerberos and DNS registration, so that the client can specify this name when mounting exports. By default, the hostname is the same as the SMB computer name or NAS server name.
`-v3`	Indicates whether NFS shares can be accessed using the NFSv4 protocol. Value is yes (default) or no.
`-v4`	Indicates whether NFS shares can be accessed using the NFSv4 protocol. Value is yes or no (default).
`-secure`	Indicates whether to enable secure NFS (with Kerberos). Value is yes or no (default). To enable secure NFS, you must also configure the NAS server Kerberos object, specify a corresponding KDC type using the `-kdcType` qualifier, and upload the keytab file (generated with kadmin).
`-kdcType`	Specifies the type of type of KDC realm to use for NFS secure. Value is one of the following: • `windows` - Use the Windows realm associated with the SMB-enabled NAS server. If you configure secure NFS using this method, SMB support cannot be deleted from the NAS server while secure NFS is enabled and configured to use the Windows realm. • `custom` - Configure a custom realm to point to any type of Kerberos realm. (Windows, MIT, Heidmal). If you configure secure NFS using this method, you must upload the keytab file to the NAS server being defined. Refer to Configure Kerberos settings on page 164 for more information.
`-username`	(Applies when the `-kdcType` is Windows.) Specifies a user name with administrative rights to register the service principal in the AD domain.
`-passwd`	(Applies when the `-kdcType` is Windows.) Specifies the AD domain administrator password.
`-passwdSecure`	Specifies the password in secure mode. The user will be prompted to input the password and the password confirmation.
`-extendedUnixCredEnabled`	Specifies whether there are more than 16 Unix groups. Valid value is 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 an NFS server on NAS server nas_1 with ID nfs_1 that supports NFSv4 and NFS secure.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/nfs create -server nas_1 -v4 yes -secure yes

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

ID = nfs_1
Operation completed successfully.
```

View an NFS server

The following command displays NFS server settings.

Format

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

Object qualifiers

Qualifier	Description
-id	Type the ID of the NFS server to view.
-server	Type the ID of the associated NAS server.
-serverName	Type the name of the associated NAS server.
-hostname	Type the hostname for the NFS server. The FDQN or short name formats are supported.

Example

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

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

1:     ID                             = nfs_1
       NAS server                     = nas_1
       Hostname                       = SATURN
       NFSv3 enabled                  = yes
       NFSv4 enabled                  = yes
       Secure NFS enabled             = yes
       Kerberos KDC type              = Windows
       Service principal name         = nfs/
SATURN.domain.lab.emc.com, nfs/SATURN
       Extended Unix credentials enabled = no
       Credentials cache retention       = 15
```

Change NFS server settings

Modify an existing NFS server.

Format

```
/net/nas/nfs [-id <value>] set [-hostname <value>] [-v3 {yes |
no}] [-v4 {yes | no}] [-secure {no | yes [-kdcType {Windows |
custom}]}] [-username <value> {-passwd <value> | -
passwdSecure}] [-extendedUnixCredEnabled {yes | no}] [-
credCacheRetention <value>]
```

Object qualifier

Qualifier	Description
`-id`	Identifies the NFS server to change.

Action qualifiers

Qualifier	Description
`-hostname`	Specifies the new hostname for the NFS server. This is used in Kerberos and DNS registration, so that the client can specify this name when mounting exports. By default, the hostname is the same as the SMB computer name or NAS server name
`-v3`	Indicates whether NFS shares can be accessed using the NFSv3 protocol. Valid values are `yes` or `no`.
`-v4`	Indicates whether NFS shares can be accessed using the NFSv4 protocol. Valid values are `yes` or `no`.
`-secure`	Indicates whether to enable secure NFS (with Kerberos). Value is yes or no. To enable secure NFS, you must also configure the NAS server Kerberos object, specify a corresponding KDC type using the `-kdcType` qualifier, and upload the keytab file (generated with kadmin).
`-kdcType`	Specifies the type of type of KDC realm to use for NFS secure. Value is one of the following: • `Windows` - Use the Windows realm associated with the SMB server configured on the NAS server. If you configure secure NFS using this method, SMB support cannot be deleted from the NAS server while secure NFS is enabled and configured to use the Windows realm. • `custom` - Configure a custom realm to point to any type of Kerberos realm (Windows, MIT, Heidmal). If you configure secure NFS using this method, you must upload the keytab file to the NAS server being defined. Refer to Configure Kerberos settings on page 164 for more information.

Qualifier	Description
-username	(Applies when the -kdcType is Windows.) Specifies a user name with administrative rights to register the service principal in the AD domain.
-password	(Applies when the -kdcType is Windows.) Specifies the AD domain administrator password.
-passwdSecure	Specifies the password in secure mode. The user will be prompted to input the password and the password confirmation.
-skipUnjoin	(Applies when the KDC realm type is Windows.) Deletes the NFS server without automatically unregistering the NFS service principals from the AD domain.
-extendedUnixCredEnabled	Specifies whether there are more than 16 Unix groups. Valid values are yes or no.
-creditCacheRetention	Specifies the amount of time (in minutes) when the credential cache refreshes or times out. Default value is 15 minutes.

Example

The following command changes the credit cache retention period for NFS server nfs_1.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/nfs -id
nfs_1 set -credCacheRetention 20
```

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

ID = nfs_1
Operation completed successfully.
```

Delete an NFS server

Delete an existing NFS server. The NFS server cannot be deleted if it has any associated resources, such as NFS shares, on the NAS server.

Format

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

Object qualifier

Qualifier	Description
-id	Identifies the NFS server to delete.

Action qualifiers

Qualifier	Description
`-username` (applies when the KDC realm type is Windows)	Specifies a user name with administrative rights to unregister the service principal from the AD domain.
`-passwd` (applies when the KDC realm type is Windows)	Specifies the AD domain administrator password.
`-passwdSecure`	Specifies the password in secure mode. The user will be prompted to input the password and the password confirmation.
`-skipUnjoin` (applies when the KDC realm type is Windows)	Deletes the NFS server without automatically unregistering the NFS service principals from the AD domain.

Example

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/nfs -id nfs_1 delete`

```
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 39 CAVA attributes

Attribute	Description
`NAS server`	Associated NAS server identifier.
`Enabled`	Indicates if CAVA is enabled. Valid values are: • `yes` • `no` **Note** Before you can enable CAVA, you must first upload a CAVA configuration file to the NAS server. See View the switches on page 29 for details on how to upload the configuration file.

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 • no **Note** Before you can enable CAVA, you must first upload a CAVA configuration file to the NAS server. See View the switches on page 29 for details on how to upload the configuration file.

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.
```

Manage Events Publishing configuration settings

Events Publishing allows third-party applications to register to receive event notification and context from the storage system when accessing file systems by using the SMB or NFS protocols. The Common Event Publishing Agent (CEPA) delivers to the application both event notification and associated context in one message. Context may consist of file metadata or directory metadata that is needed to decide business policy.

You must define at least one event option (pre-, post-, or post-error event) when Events Publishing is enabled.

- Pre-event notifications are sent before processing an SMB or NFS client request.
- Post-event notifications are sent after a successful SMB or NFS client request.
- Post-error event notifications are sent after a failed SMB or NFS client request.

Table 40 Events Publishing attributes

Attributes	**Description**
`NAS server`	Identifies the associated NAS server.
`Enabled`	Identifies whether Events Publishing is enabled on the NAS Server. Valid values are: • `yes` • `no` (default)
`Pre-event failure policy`	Policy applied when a pre-event notification fails. Valid values are: • `ignore` (default) - indicates that when a pre-event notification fails, it is acknowledged as being successful. • `deny` - indicates that when a pre-event notification fails, the request of the SMB or NFS client is not executed by the storage system. The client receives a 'denied' response.
`Post-event failure policy`	Policy applied when a post-event notification fails. The policy is also applied to post-error events. Valid values are: • `ignore` (default) - continue and tolerate lost events. • `accumulate` - continue and use a persistence file as a circular event buffer for lost events. • `guarantee` - continue and use a persistence file as a circular event buffer for lost events until the buffer is filled, and then deny access to file systems where Events Publishing is enabled. • `deny` - on CEPA connectivity failure, deny access to file systems where Events Publishing is enabled.
`HTTP port`	HTTP port number for connectivity to the CEPA server. The default value is 12228. The HTTP protocol is used to connect to CEPA servers. It is not protected by a username or password.

Table 40 Events Publishing attributes (continued)

Attributes	Description
`HTTP enabled`	Identifies whether connecting to CEPA servers by using the HTTP protocol is enabled. When enabled, a connection by using HTTP is tried first. If HTTP is either disabled or the connection fails, then connection through the MS-RPC protocol is tried if all CEPA servers are defined by a fully-qualified domain name (FQDN). When an SMB server is defined in a NAS server in the Active Directory (AD) domain, the NAS server's SMB account is used to make an MS-RPC connection. Valid values are: • `yes` (default) • `no`
`Username`	When using the MS-RPC protocol, name of a Windows user allowed to connect to CEPA servers.
`Password`	When using the MS-RPC protocol, password of the Windows user defined by the username.
`Heartbeat`	Time interval (in seconds) between scanning CEPA servers to detect their online or offline status. The default is 10 seconds. The range is from 1 through 120 seconds.
`Timeout`	Time in ms to determine whether a CEPA server is offline. The default is 1,000 ms. The range is from 50 ms through 5,000 ms.
`Health state`	Health state of Events Publishing. The health state code appears in parentheses. Valid values are: • `OK (5)` - the Events Publishing service is operating normally. • `OK_BUT (7)` - some CEPA servers configured for the NAS server cannot be reached. • `Minor failure (15)` - the Events Publishing service is not functional. • `Major failure (20)` - all CEPA servers configured for the NAS server cannot be reached.
`Health details`	Additional health information. See Appendix A, Reference, for details.

View CEPA configuration settings

View details about CEPA configuration settings.

Format

```
/net/nas/event/config [-server <value>] show
```

Object qualifier

Qualifier	Description
`-server`	Identifies the associated NAS server.

Example

The following example displays the CEPA settings.

```
uemcli /net/nas/event/config -server nas_1 show -detail
```

```
Storage system address: 10.1.2.100
Storage system port: 443
HTTPS connection

1:      NAS server                 = nas_1
        Enabled                    = yes
        Pre-event failure policy   = ignore
        Post-event failure policy = ignore
        HTTP port                  = 12228
        HTTP enabled               = yes
        Username                   = user1
        Heartbeat                  = 10s
        Timeout                    = 1000ms
        Health state               = OK (5)
        Health details             = The Events Publishing Service is
operating normally.
```

Change CEPA configuration settings

Modify the Events Publishing configuration. When you create a NAS server, an Events Publishing configuration object is automatically created with default values.

Format

```
/net/nas/event/config –server <value> set [-enabled {yes | no}]
[-preEventPolicy {ignore | deny}] [-postEventPolicy {ignore |
accumulate | guarantee | deny}] [-httpPort <value>] [-
httpEnabled {yes | no}] [-username <value> {-passwd <value> | -
passwdSecure}] [-heartbeat <value>] [-timeout <value>]
```

Object qualifier

Qualifier	Description
`-server`	Identifies the associated NAS server.

Action qualifiers

Qualifier	Description
`-enabled`	Identifies whether Events Publishing is enabled on the NAS Server. Valid values are: • `yes` • `no` (default)
`-preEventPolicy`	Identifies the policy applied when a pre-event notification fails. Valid values are: • `ignore` (default) - indicates that when a pre-event notification fails, it is acknowledged as being successful. • `deny` - indicates that when a pre-event notification fails, it is acknowledged with a 'denied' answer.

Qualifier	Description
`-postEventPolicy`	Identifies the policy applied when a post-event notification fails. The policy is also applied to post-error events. Valid values are: • `ignore` (default) - continue and tolerate lost events. • `accumulate` - continue and use a persistence file as a circular event buffer for lost events. • `guarantee` - continue and use a persistence file as a circular event buffer for lost events until the buffer is filled, and then deny access to file systems where Events Publishing is enabled. • `deny` - on CEPA connectivity failure, deny access to file systems where Events Publishing is enabled.
`-httpPort`	HTTP port number used for connectivity to the CEPA server. The default value is 12228. The HTTP protocol is used to connect to CEPA servers. It is not protected by a username or password.
`-httpEnabled`	Specifies whether connecting to CEPA servers by using the HTTP protocol is enabled. When enabled, a connection by using HTTP is tried first. If HTTP is either disabled or the connection fails, then connection through the MS-RPC protocol is tried if all CEPA servers are defined by a fully-qualified domain name (FQDN). The SMB account of the NAS server in the Active Directory domain is used to make the connection by using MS-RPC. Valid values are (case insensitive): • `yes` (default) • `no`
`-username`	Name of a Windows user who is allowed to connect to CEPA servers. **Note** To ensure that a secure connection (by using the Microsoft RPC protocol) is used, you must disable HTTP by setting –`httpEnabled=no`.
`-passwd`	Password of the Windows user defined by the username.
`-passwdSecure`	Specifies the password in secure mode. The user is prompted to specify the password.
`-heartbeat`	Time interval between scanning CEPA servers (in seconds) to detect their online or offline status. The default is 10 seconds. The range is from 1 through 120 seconds.
`-timeout`	Time in ms to determine whether a CEPA server is offline. The default is 1,000 ms. The range is from 50 ms through 5,000 ms.

Example

The following command enables Events Publishing and sets the post-event policy to `accumulate`.

```
uemcli /net/nas/event/config -server nas_1 set -enabled yes -postEventPolicy accumulate
```

```
Storage system address: 10.1.2.100
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage CEPA pool configuration settings

Event pools configure the types of events published by the NAS Server, and the addresses of CEPA servers.

Events Publishing must be enabled for both the NAS server and the file system. Certain types of events can be enabled for either the NFS protocol, the SMB protocol, or both NFS and SMB on a file system basis.

Table 41 CEPA pool attributes

Attributes	Description
`ID`	Identifies the Events Publishing pool.
`NAS server`	Identifies the associated NAS server.
`Name`	Identifies the Events Publishing pool name.
`Addresses`	Addresses of the CEPA servers. A CEPA pool allows using IPv4, IPv6, and FQDN addresses.
`Replication sync`	Applicable only when the NAS server is replicated through a replication session. Valid values are: • `Not replicated` • `Auto synchronized` – indicates that the Events Publishing pool servers list is automatically synchronized over the replication session to the destination. Any modify and delete operations on the source are automatically reflected on the destination. • `Overridden` – indicates that the Events Publishing pool servers list is manually modified or overridden on the destination side. When an Events Publishing pool servers list is created on the source of a replication, it is auto-synchronized to the destination NAS server. IP address changes or deletions from the Events Publishing pool servers list on a source Events Publishing server have no effect on overridden Events Publishing pool servers on the destination.
`Source addresses`	Addresses of the CEPA servers defined on the replication source. A CEPA pool allows using IPv4, IPv6, and FQDN addresses.

Table 41 CEPA pool attributes (continued)

Attributes	Description
`Pre-events`	Lists the selected pre-events. The NAS server sends a request event notification to the CEPA server before an event occurs and processes the response. The valid events are defined in the table that follows.
`Post-events`	Lists the selected post-events. The NAS server sends a notification after an event occurs. The valid events are defined in the table that follows.
`Post-error events`	Lists the selected post-error events. The NAS server sends notification after an event generates an error. The valid events are defined in the table that follows.

Table 42 Event descriptions

Value	Definition	Protocol
`OpenFileNoAccess`	Sends a notification when a file is opened for a change other than read or write access (for example, read or write attributes on the file).	• SMB/CIFS • NFS (v4)
`OpenFileRead`	Sends a notification when a file is opened for read access.	• SMB/CIFS • NFS (v4)
`OpenFileReadOffline`	Sends a notification when an offline file is opened for read access.	• SMB/CIFS • NFS (v4)
`OpenFileWrite`	Sends a notification when a file is opened for write access.	• SMB/CIFS • NFS (v4)
`OpenFileWriteOffline`	Sends a notification when an offline file is opened for write access.	• SMB/CIFS • NFS (v4)
`OpenDir`	Sends a notification when a directory is opened.	SMB/CIFS
`FileRead`	Sends a notification when a file read is received over NFS.	NFS (v3/v4)
`FileWrite`	Sends a notification when a file write is received over NFS.	NFS (v3/v4)
`CreateFile`	Sends a notification when a file is created.	• SMB/CIFS • NFS (v3/v4)
`CreateDir`	Sends a notification when a directory is created.	• SMB/CIFS • NFS (v3/v4)
`DeleteFile`	Sends a notification when a file is deleted.	• SMB/CIFS • NFS (v3/v4)
`DeleteDir`	Sends a notification when a directory is deleted.	• SMB/CIFS

Table 42 Event descriptions (continued)

Value	Definition	Protocol
		- NFS (v3/v4)
`CloseModified`	Sends a notification when a file is changed before closing.	- SMB/CIFS - NFS (v4)
`CloseUnmodified`	Sends a notification when a file is not changed before closing.	- SMB/CIFS - NFS (v4)
`CloseDir`	Sends a notification when a directory is closed.	SMB/CIFS
`RenameFile`	Sends a notification when a file is renamed.	- SMB/CIFS - NFS (v3/v4)
`RenameDir`	Sends a notification when a directory is renamed.	- SMB/CIFS - NFS (v3/v4)
`SetAclFile`	Sends a notification when the security descriptor (ACL) on a file is changed.	SMB/CIFS
`SetAclDir`	Sends a notification when the security descriptor (ACL) on a directory is changed.	SMB/CIFS
`SetSecFile`	Sends a notification when a file security change is received over NFS.	NFS (v3/v4)
`SetSecDir`	Sends a notification when a directory security change is received over NFS.	NFS (v3/v4)

Create a CEPA pool

Create a CEPA pool.

Format

```
/net/nas/event/pool create -server <value> -name <value> -addr
<value> [-preEvents <value>] [-postEvents <value>] [-
postErrEvents <value>]
```

Action qualifiers

Qualifier	Description
`-server`	Identifies the associated NAS server.
`-name`	Specifies a CEPA pool name. The name must be unique for each NAS server.
`-addr`	Specifies a comma-separated list of addresses of the CEPA servers. You can specify IPv4, IPv6, and FQDN addresses.
`-preEvents`	Specifies the comma-separated list of pre-events.
`-postEvents`	Specifies the comma-separated list of post-events.
`-postErrEvents`	Specifies the comma-separated list of post-error events.

Example

The following command creates a CEPA pool and a list of post events for which to be notified.

uemcli /net/nas/event/pool create -server nas_1 -name mypool1 -addr 10.1.2.100 -postEvents CreateFile,DeleteFile

```
Storage system address: 10.1.2.100
Storage system port: 443
HTTPS connection

ID = cepa_pool_1
Operation completed successfully.
```

View CEPA pool settings

View details about a CEPA pool.

Format

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

Object qualifier

Qualifier	Description
-id	Identifies the Events Publishing pool.
-server	Identifies the associated NAS server.
-name	Identifies the Events Publishing pool name.

Example

The following command displays information about a CEPA pool.

uemcli /net/nas/event/pool -server nas_1 show

```
Storage system address: 10.1.2.100
Storage system port: 443
HTTPS connection

1:     ID                  = cepa_pool_1
       NAS server          = nas_1
       Name                = MyCepaPool
       Addresses           = 10.1.2.2
       Pre-events          =
       Post-events         = CreateFile, DeleteFile
       Post-error events   =
```

Change CEPA pool settings

Modify settings for an existing Events Publishing pool.

Format

/net/nas/event/pool -id *<value>* set [-name *<value>*] [-addr *<value>*] [-preEvents *<value>*] [-postEvents *<value>*] [-postErrEvents *<value>*] [-replSync {auto | overridden}]

Object qualifier

Qualifier	Description
`-id`	Identifies the Events Publishing pool.

Action qualifiers

Qualifier	Description
`-name`	Specifies a CEPA Pool name. The name is unique for any specified NAS server.
`-addr`	Specifies a comma-separated list of addresses of the CEPA servers. A CEPA pool allows IPv4, IPv6, and FQDN addresses.
`-preEvents`	Specifies the comma-separated list of pre-events.
`-postEvents`	Specifies the comma-separated list of post-events.
`-postErrEvents`	Specifies the comma separated list of post-error events.
`-replSync`	Applicable only when the NAS server is operating as a replication destination. The valid values are: • `auto` – indicates that the Events Publishing pool servers list is automatically synchronized over the replication session to the destination. Any change and delete operations on the source are automatically reflected on the destination. • `overridden` – indicates that the Events Publishing pool servers list is manually changed or overridden on the destination side. When a replicated Events Publishing pool servers list is created on the source Events Publishing server, it is auto-synchronized to the destination. Changes or deletions of IP addresses from the Events Publishing pool servers list on a source Events Publishing service have no effect on an overridden Events Publishing pool servers list on the destination.

Example

The following command changes the name for a CEPA pool.

`uemcli /net/nas/event/pool -id cepa_pool_1 set -name TestCepaPool`

```
Storage system address: 10.1.2.100
Storage system port: 443
HTTPS connection

ID = cepa_pool_1
Operation completed successfully.
```

Delete a CEPA pool

Deletes a CEPA pool.

Before you begin

The Events Publishing service requires at least one CEPA pool. If you delete the last CEPA pool, the Events Publishing service becomes disabled.

Format

`/net/nas/event/pool [{-id <value> | -name <value>}] delete`

Object qualifiers

Qualifier	Description
`-id`	Identifies the Events Publishing pool.
`-name`	Identifies the Events Publishing pool name.

Example

The following command deletes a CEPA pool.

`uemcli /net/nas/event/pool -id cepa_pool_1 delete`

```
Storage system address: 10.1.2.100
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manage VMware NAS protocol endpoint servers

VMware protocol endpoint servers are NFS-based NAS servers enabled to provide an I/O path from the VMware host to it's respective File VVol datastore on the storage system.

When creating a NAS protocol endpoint server, you can choose which IP address the NAS PE will use from the list of IP interfaces already created for the NAS server. It is recommended that you enable at least two NAS servers for VVols, one on each SP, for high availability. The system will select one of these NAS PEs automatically based on which will maximize throughput.

Table 43 Protocol endpoint server attributes

Attribute	Description
`ID`	VMware protocol endpoint identifier.
`NAS server`	Identifier of the associated NAS server for NAS PEs.
`NAS server interface`	Identifier of the NAS server IP interface to be used by the VMware NAS protocol endpoint server.

Note

Only one VMware protocol endpoint server per NAS server is supported.

Create protocol endpoint servers

Create VMware protocol endpoints servers for File VVols.

Format

```
/net/nas/vmwarepe create [-async] {-server <value> | -serverName <value>} -if <value>
```

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-server`	Type the identifier of the NAS server.
`-serverName`	Type the name of the NAS server.
`-if`	Type the name of the identifier for the NAS IP interface to be used by the VMware protocol endpoint server.

Example

The following example creates a protocol endpoint server on NAS server "nas_1" with the IP interface "if_1".

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/vmwarepe create -server nas_1 -if if_ 1
```

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

ID = PES_0
Operation completed successfully.
```

View VMware protocol endpoint servers

View VMware protocol endpoints servers for File VVols.

Format

```
/net/nas/vmwarepe [{-id <value> | -server <value> | -serverName <value>}] show
```

Action qualifier

Qualifier	Description
`-id`	Type the identifier of the NAS protocol endpoint server.
`-server`	Type the identifier of the associated NAS server.
`-serverName`	Type the name of the associated NAS server.

Example

The following example shows the details for all of the VMware protocol endpoint servers on the system.

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

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

```
1:     ID                   = PES_0
       NAS server           = nas_1
       NAS server interface = if_1
```

Delete protocol endpoint servers

Delete a VMware protocol endpoints server.

Format

`/net/nas/vmwarepe -id <value> delete [-async] [-force]`

Object qualifiers

Qualifier	Description
`-id`	Type the identifier or the VMware protocol endpoint server to be deleted.

Action qualifiers

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-force`	Unconditionally removes all VMware NAS protocol endpoints using the VMware protocol endpoint server and unbinds all virtual volumes using the protocol endpoint server.

Example

The following example deletes VMware NAS protocol endpoint server "PES_0".

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/vmwarepe –id PES_0 delete`

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

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 291 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 44 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

The show action command on page 23 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 45 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

The show action command on page 23 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 46 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 194 explains how to configure reverse CHAP authentication between iSCSI hosts and nodes.

The following table lists the attributes for iSCSI nodes.

Table 47 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. **Note** Manage network interfaces on page 213 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 23 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 48 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.
`Protocols`	Types of protocols the port supports. Value is one of the following: • `mgmt` — Management interface. • `file` — Network interface for Windows (SMB) and Linux/UNIX (NFS) storage. • `iscsi` — iSCSI interface for iSCSI storage. Manage network interfaces on page 213 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. **Note** This can display as either a comma-separate list of exact values (if there is an iSCSI interface on the port), or an interval defined by the minimum or maximum values, such as 1280-9216.

Table 48 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 224 explains how to configure link aggregations on the SP ports.
Connector type	Physical connector type. Valid values are: • unknown • RJ45 • LC • MiniSAS_HD • CopperPigtail • NoSeparableConnector
MAC address	Unique identifier assigned to a network device for communications on a network segment.
SFP supported speeds	List of supported speed values of the inserted Small Form-factor Pluggable.
SFP supported protocols	List of supported protocols of the inserted Small Form-factor Pluggable. Valid values are: • unknown • FibreChannel • Ethernet • SAS

View Ethernet port settings

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

Note

The show action command on page 23 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 -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/port/eth show -detail
```

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

1:     ID                       = spa_eth2
       Name                     = SP A Ethernet Port 2
       SP                       = spa
       Protocols                = file, net, iscsi
       MTU size                 = 4500
       Requested MTU size       = 4500
       Available MTU sizes      = 1280-9216
       Linux device name        = eth2
       Speed                    = 1 Gbps
       Requested speed          = auto
       Available speeds         = 1 Gbps, 10 Gbps, 100 Mbps, auto
       Health state             = OK (5)
       Health details           = "The port is operating normally."
       Aggregated port ID       = None
       FSN port ID              = None
       Connector type           = RJ45
       MAC address              = 00:60:16:7A:7F:CF
       SFP supported speeds     =
       SFP supported protocols  =

2:     ID                       = spa_eth3
       Name                     = SP A Ethernet Port 3
       SP                       = spa
       Protocols                = file, net, iscsi
       MTU size                 = 1500
       Requested MTU size       = 1500
       Available MTU sizes      = 1500, 9000
       Linux device name        = eth3
       Speed                    = 1 Gbps
       Requested speed          = auto
       Available speeds         = 1 Gbps, 10 Gbps, 100 Mbps, auto
       Health state             = OK (5)
       Health details           = "The port is operating normally."
       Aggregated port ID       = None
       FSN port ID              = None
       Connector type           = RJ45
       MAC address              = 00:60:16:7A:7F:CE
       SFP supported speeds     =
       SFP supported protocols  =
```

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: • If an Ethernet port carries File interfaces only, the MTU size can be set to a custom value between 1280 and 9216. • If an Ethernet port carries iSCSI interfaces, the allowed MTU sizes are 1500 and 9000. Specific I/O modules may also restrict allowed range for MTU size value. The MTU size values of 1500 bytes (default) and 9000 bytes (jumbo frame) are supported by all interfaces and I/O modules.
`-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 49 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. Valid values are: - spa - spb
Speed	Current link speed of the port.
Health state	Health state of the port. The health state code appears in parentheses. Valid values are: - 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 Health details on page 702 for health information details.
Connector type	Physical connector type. Valid values are: - unknown - RJ45 - LC - MiniSAS_HD - CopperPigtail - NoSeparableConnector

View SAS settings

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

Note

The show action command on page 23 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 50 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.
`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:

Table 50 FC port attributes (continued)

Attribute	Description
	• unknown • RJ45 • LC • MiniSAS_HD • CopperPigtail • NoSeparableConnector
SFP supported speeds	List of supported speed values of the inserted Small Form-factor Pluggable.
SFP supported protocols	List of supported protocols of the inserted Small Form-factor Pluggable. Valid values are: • unknown • FibreChannel • Ethernet • SAS
Replication capability	Type of replication capability. Valid values are: • Sync replication • RecoverPoint

View FC port settings

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

Format

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

Object qualifier

Qualifier	Description
-id	Type the ID of the port.

Example

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

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

1:      ID                        = spa_fc4
        Name                      = SP A FC Port 4
        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        = 4 Gbps, 8 Gbps, 16 Gbps, auto
        Health state            = OK (5)
        Health details          = "The port is operating normally."
        SFP supported speeds    = 4 Gbps, 8 Gbps, 16 Gbps
        SFP supported protocols = FibreChannel
        Replication capability  = Sync replication
        SFP supported mode      = Multimode
```

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 -d 10.0.0.1 -u Local/joe -p MyPassword456! /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.
```

Manage uncommitted ports

This command is used to manage uncommitted network ports.

Uncommitted ports must be initialized in order to be used by the system. Use the CLI to view information on the uncommitted and removed system Small Form-factor Pluggable (SFP) ports.

Table 51 Uncommitted port attributes

Attribute	Description
ID	Port identifier.
Name	Port name.

Table 51 Uncommitted port attributes (continued)

Attribute	Description
SP	Storage processor on which the port resides.
Health state	Current health state of the port. Valid states are: - Unknown (0) — Status is unknown. - OK (5)—The Uncommitted port is uninitialized. It needs to be committed before it can be used. - OK (5)—The Small Form-factor Pluggable (SFP) module in this Uncommitted port has been removed. Since the port is not in use, no action is required.
Health details	Additional health information.
Connector type	Physical connector type associated with the uncommitted port. Valid values are: - unknown - RJ45 - LC - MiniSAS_HD - CopperPigtail - NoSeparableConnector
SFP supported speeds	List of supported speed values of the inserted SFP.
SFP supported protocols	List of supported protocols of the inserted SFP. Valid values are: - unknown - FibreChannel - Ethernet

View uncommitted ports

Use this command to view a list of uncommitted ports on the system.

View details about uncommited ports.

Format

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

Object qualifier

Qualifier	Description
-id	Type the ID of the port.

Example

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/port/unc show -detail`

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


1:    ID                      = spb_unc5
      Name                    = SP B Uncommitted Port 5
      SP                      = spb
      Health state            = OK (5)
      Health details          = "The Small Form-factor Pluggable
(SFP) module in this Uncommitted port has been removed. Since the
port is not in use, no action is required."
      Connector type          = LC
      SFP supported speeds    =
      SFP supported protocols =

2:    ID                      = spa_unc5
      Name                    = SP A Uncommitted Port 5
      SP                      = spa
      Health state            = OK (5)
      Health details          = "The Uncommitted port is
uninitialized. It needs to be committed before it can be used."
      Connector type          = LC
      SFP supported speeds    = 10 Gbps
      SFP supported protocols = Ethernet

3:    ID                      = spb_iom_1_unc0
      Name                    = SP B I/O Module 1 Uncommitted Port 0
      SP                      = spb
      Health state            = OK (5)
      Health details          = "The Uncommitted port is
uninitialized. It needs to be committed before it can be used."
      Connector type          = RJ45
      SFP supported speeds    =
      SFP supported protocols =
```

Manage 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 52 Interface attributes

Attribute	Description
`IP protocol version`	IP protocol version. Valid values are: ● `ipv4`

Table 52 Interface attributes (continued)

Attribute	Description
	• `ipv6`
`Address origin`	IP settings origin. Valid values are: • `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 network 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.

The system configures each interface on a pair of symmetrical SP ports. The interface can be moved between SPs. You have the option of indicating which SP the interface will use, either a physical port or a link aggregation port. You also have the option of specifying a virtual LAN (VLAN) ID, for communicating with VLAN networks.

Each interface is identified by an ID.

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

Table 53 Interface attributes

Attribute	Description
`ID`	ID of the interface.
`Type`	Interface type. Value is one of the following: • `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.
`Health state`	A numerical value indicating the health of the system. Value is one of the following: • `Unknown (0)` • `OK (5)` • `OK BUT (7)` • `Degraded/Warning (10)` • `Minor failure (15)` • `Major failure (20)`

Table 53 Interface attributes (continued)

Attribute	Description
`Health details`	Additional health information.

Create interfaces

Create an interface.

Format

```
/net/if create [ -async ] [-vlanId <value>] -type { iscsi |
replication} -port <value> -addr <value> [-netmask <value>] [-
gateway <value>]
```

Action qualifier

Qualifier	Description
`-async`	Run the creation operation in asynchronous mode.
`-type`	Specify the interface type. Value is one of the following: • `iscsi` — Interface for iSCSI storage. • `replication` — Interface for replication-related data or management traffic.
`-port`	Specify the ID of the SP port or link aggregation that will use the interface. **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.
`-vlanId`	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 1–4095. **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`	Specify 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`	Specify the subnet mask for the interface.

Qualifier	Description
	Note This qualifier is not required if the prefix length is specified in the -addr attribute.
`-gateway`	Specify the gateway for the interface. **Note** This qualifier configures the default gateway for the specified port's SP.

Example

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.
```

View interfaces

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

Note

The show action command on page 23 explains how to change the output format.

Format

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

Object qualifier

Qualifier	Description
`-id`	Type the ID of an interface.
`-port`	Type the port the interface is associated with.
`-type`	Specify the type of the interface. Valid values are: • `iscsi` • `replication`

Example

The following command displays the details of all interfaces on the system.

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

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

1:      ID                       = if_0
        Type                     = file
        NAS server               = nas_0
        Port                     = eth0_spa
        VLAN ID                  = 0
        IP address               = 3ffe:80c0:22c:4e:a:0:2:7f/64
        Subnet mask              =
        Gateway                  = fe80::20a8bff:fe5a:967c
        IPv4 mode                =
        IPv4 address             =
        IPv4 subnet mask         =
        IPv4 gateway             =
        IPv6 mode                = static
        IPv6 address             = 3ffe:80c0:22c:4e:a:0:2:7f/64
        IPv6 link-local address =
        IPv6 gateway             = fe80::20a8bff:fe5a:967c
        MAC address              = EA:3E:22:3F:0C:62
        SP                       = spa
        Preferred                = yes

2:      ID                       = if_1
        Type                     = file
        NAS server               = nas_1
        Port                     = eth1_spb
        VLAN ID                  = 1
        IP address               = 192.168.1.2
        Subnet mask              = 255.255.255.0
        Gateway                  = 192.168.1.254
        IPv4 mode                = static
        IPv4 address             = 192.168.1.2
        IPv4 subnet mask         = 255.255.255.0
        IPv4 gateway             = 192.168.1.254
        IPv6 mode                =
        IPv6 address             =
        IPv6 link-local address =
        IPv6 gateway             =
        MAC address              = EA:3E:22:21:7A:78
        SP                       = spa
        Preferred                = yes

3:      ID                       = if_2
        Type                     = replication
        NAS server               =
        Port                     = eth1_spb
        VLAN ID                  =
        IP address               = 10.103.75.56
        Subnet mask              = 255.255.248.0
        Gateway                  = 10.103.72.1
        IPv4 mode                = static
        IPv4 address             = 10.103.75.56
        IPv4 subnet mask         = 255.255.248.0
        IPv4 gateway             = 10.103.72.1
        IPv6 mode                =
        IPv6 address             =
        IPv6 gateway             =
        MAC address              = EA:3E:22:6D:BA:40
        SP                       = spb
        Preferred                = no
```

Change interface settings

Change the settings for an interface.

Format

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

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.

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.

NOTICE

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 destined for a non-local subnet so it can reach its destination, whether that destination is a network or host. A static IP route is a host, network, or default route that is configured manually.

The system selects a route in order from most specific to least specific, as follows:

1. Host (most specific)
2. Network
3. Default (least specific)

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 54 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 216 explains how to view the network interface IDs.
`Route type`	Type of route. Valid 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. Valid values are: • 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.
`Health state`	A numerical value indicating the health of the system. Valid values are: • Unknown (0) • OK (5) • OK BUT (7) • Degraded/Warning (10) • Minor failure (15) • Major failure (20)
`Health details`	Additional health information. See Appendix A, Reference, for health information details.

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 216 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 network route for interface if_1 to reach the 10.64.74.x subnet using gateway 10.64.74.1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/route create –if IF_1 -type net -target 10.64.200.10 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 23 explains how to change the output format.

Format

```
/net/route [ {-id <value> | -if <value>} ] show
```

Object qualifier

Qualifier	Description
`-id`	Specifies the ID of a route.
`-if`	Specifies the network interface for which you want to return routes.

Example

The following command displays details of the IP routes RT_1, RT_2, and RT_3:

```
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_1
        Type         = net
        Target       = 10.64.74.10
        Netmask      = 255.255.255.0
        Gateway      = 10.0.0.1
        Interface    = IF_1
        Health state = OK (5)

2:      ID           = RT_2
        Type         = default
        Target       =
        Netmask      =
        Gateway      = 10.64.74.2
        Interface    = IF_2
        Health state = OK (5)

3:      ID           = RT_3
        Type         = host
        Target       = 10.64.74.168
        Netmask      =
        Gateway      = 10.0.0.3
        Interface    = IF_3
        Health state = OK (5)
```

Change IP routes

Modify an existing IP route.

Format

```
/net/route set route -id <value> set [-type {default | host |
net}] [-target <value> [-netmask <value>]] [-gateway <value>]
```

Object qualifier

Qualifier	Description
`-id`	Identifies the route object.

Action qualifier

Qualifier	Description
`-type`	Specify the type of route. Only one default IPv4 route instance is allowed. Valid values are (case-insensitive): • `default` — System uses the default gateway when it cannot find a more specific host or network route. • `host` — Create a route to a host. • `net` — Create a route to a subnet.
`-target`	Specify the destination IP address or a range of IP addresses. If the route type is: • *host*, the value is an IP address of the host. • *net*, the value is a subnet IP address with the following format: `<IPv4 address>/[<prefix length>]` or `<IPv6 address>/[<prefix length>].` Default prefix length is 24 for `IPv4 address` and 64 for `IPv6 address`. Valid values are: • For a default route, the system uses the IP address specified for `–gateway`. • For a host route, specify the IP address of a target host. • For a net route, specify 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`	Specify the gateway IP address for the route.

Example

The following command changes the target IP address to 10.64.200.11, the netmask to 255.255.255.0, and the gateway to 10.64.74.2 for IP route RT_1:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/route -id RT_1 set -target 10.64.200.11 -netmask 255.255.255.0 -gateway 10.64.74.2`

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

ID = RT_1
Operation completed successfully.
```

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 55 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. Valid values are: - `SPA` - `SPB`
`MTU size`	Maximum transmission unit (MTU) packet size (in bytes) for the linked ports. Default is 1500 bytes per packet.
`Linux device name`	Linux network device name.
`FSN port ID`	ID of the FSN port to which the link aggregation belongs, if it is part of an FSN.
`Available MTU size`	List of available MTU sizes. **Note** This displays as an interval defined by the minimum and maximum values, for example: 1280-9216.
`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. - `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.

Table 55 Link aggregation 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.

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. The MTU size can be set to a custom value between 1280 and 9216. Specific I/O modules may restrict allowed range for MTU size value. The MTU size values of 1500 bytes (default) and 9000 bytes (jumbo frame) are supported by all interfaces and I/O modules.

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.

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 -detail`

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

1:     ID                    = spa_la_0_2
       SP                    = spa
       Ports                 = spa_iom_0_eth2, spa_iom_0_eth3
       FSN port ID           = None
       MTU size              = 3456
       Available MTU sizes = 1280-9216
       Linux device name    = bond12
       Health state         = OK (5)
       Health details       = "The component is operating normally.
No action is required."
       Operational status   =

2:     ID                    = spb_la_0_2
       SP                    = spb
       Ports                 = spb_iom_0_eth2, spb_iom_0_eth3
       FSN port ID           = None
       MTU size              = 3456
       Available MTU sizes = 1280-9216
       Linux device name    = bond12
       Health state         = OK (5)
       Health details       = "The component is operating normally.
No action is required."
       Operational status   =
```

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. The MTU size can be set to a custom value between 1280 and 9216. Specific I/O modules may restrict allowed range for MTU size value. The MTU size values of 1500 bytes (default) and 9000 bytes (jumbo frame) are supported by all interfaces and I/O modules.

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 Fail-safe networking (physical deployments only)

Learn about Fail-safe networking (FSN) and which attributes are used to manage FSN in the CLI.

A Fail-Safe Network (FSN) is a high-availability feature that extends link failover into the network by providing switch-level redundancy. An FSN appears as a single link with a single MAC address and potentially multiple IP addresses. An FSN can be a port, a link aggregation, or any combination of the two. An FSN adds an extra layer of availability to link aggregations alone. Link aggregations provide availability in the event of a port failure. FSNs provide availability in the event of a switch failure. Each port or link aggregation is considered as a single connection. Only one connection in an FSN is active at a time. All the connections making up the FSN share a single hardware (MAC) address.

If the system detects a failure of the active connection, it will automatically switch to the standby connection in the FSN. That new connection assumes the network identity of the failed connection, until the primary connection is available again. You can designate which connection is the primary port/connection. To ensure connectivity in the event of a hardware failure, create FSN devices on multiple I/O modules or onboard ports. The FSN components are connected to different switches. If the network switch for the active connection fails, the FSN fails over to a connection using a different switch, thus extending link failover out into the network.

When replicating from one Unity system to another, configure the FSN the same way on both systems as a best practice. You will need to manually configure the FSN on the destination before setting up replication. Otherwise, if you set up the FSN on the destination after replication is configured, you will need to use the override option to select the FSN as the interface for the destination NAS server.

Note

A NAS server IP interface should be build on the highest level logical device. If you want to repurpose a port or link aggregation currently used as a NAS server IP interface for an FSN, you will need to remove the IP interface from the NAS server, create the FSN, and reassign the IP interface to the FSN device.

Table 56 FSN attributes

Attribute	Description
`ID`	ID of the Fail-Safe Networking port.
`SP`	Storage processor the FSN is on.
`MTU size`	Maximum Transmission Unit (MTU) size.
`Available MTU sizes`	List of available MTU sizes. **Note** This displays as an interval defined by the minimum and maximum values, for example: 1280-9216.
`Linux device name`	Name of the Linux network device.
`Primary port`	ID of the primary port used in the FSN. The primary port cannot be removed.
`Secondary ports`	Comma-separated list of the other secondary ports in the FSN. This includes both link aggregations and ethernet ports.
`Active port`	ID of the active port for the FSN.
`Health state`	The health state of the FSN. Valid values are: • `OK (5)` — The FSN is operating normally, or the active port of the FSN has changed. • `Degraded/Warning (10)` — Performance of the FSN has degraded. • `Minor failure (15)` — An FSN port link is down. • `Major failure (20)` — An FSN port is missing ports, or an FSN port is not symmetrical.
`Health details`	Detailed health information for the FSN.

Create an FSN

Use the CLI to create a fail-safe network.

Create a fail-safe network using two or more ports or link aggregations.

Format

```
/net/fsn create -primaryPort <value> -secondaryPorts <value> [-
mtuSize <value>]
```

Action qualifier

Qualifier	Description
`-primaryPort`	Type the ID of the primary port for the FSN. This can be either an ethernet port or link aggregation.

Qualifier	Description
`-secondaryPorts`	Type the comma-separated list of additional port or link aggregation IDs to be included in the FSN.
`-mtuSize`	Optionally, type the Maximum Transmission Unit size for the FSN. The MTU must be in the range allowed for all of the ports included in the FSN. The MTU size can be set to a custom value between 1280 and 9216. Specific I/O modules may restrict allowed range for MTU size value. The MTU size values of 1500 bytes (default) and 9000 bytes (jumbo frame) are supported by all interfaces and I/O modules.

Example

The following example creates an FSN where the primary port is a single ethernet port, and the secondary ports include a link aggregation and additional single ethernet port.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/fsn create -
primaryPort spa_eth0 -secondaryPorts "spa_la_2,spa_eth3"
```

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

ID = spa_fsn_0
ID = spb_fsn_0

Operation completed successfully.
```

View FSN settings

Review the list and details of each FSN on the system.

Format

`/net/fsn [-id <value>] show`

Object qualifier

Qualifier	Description
`-id`	Type the ID for the FSN port for which you would like to view details. Do not specify to see details for all FSNs on the system.

Example

The following example shows the details of all the FSNs on the system.

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

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

1:    ID                   = spa_fsn_0_1
      SP                   = spa
      Primary port         = spa_iom_0_eth1
      Secondary ports      = spa_la_2
      Active port          = spa_iom_0_eth1
      MTU size            = 1500
      Available MTU sizes = 1500,9000
      Health state        = OK (5)
      Health details      = "FSN port is operating normally."

2:    ID                  = spb_fsn_0_1
      SP                  = spb
      Primary port        = spb_iom_0_eth1
      Secondary ports     = spb_la_2
      Active port         = spb_iom_0_eth1
      MTU size            = 1500
      Available MTU sizes = 1500,9000
      Health state        = OK (5)
      Health details      = "FSN port is operating normally."
```

Change an FSN

Make changes to an existing FSN.

Change a fail-safe network by modifying the included secondary ports or MTU sizes.

Format

```
/net/fsn -id <value> set [-secondaryPorts <value>] [-mtuSize
<value>]
```

Object qualifier

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

Action qualifier

Qualifier	Description
-secondaryPorts	Type the list of full IDs of the physical ports and/or link aggregation ports for the FSN. Remove any from the list you wanted deleted from the FSN, and add any you want included.
-mtuSize	Type the new Maximum Transmission Unit (MTU) size for the FSN. The MTU must be in the range allowed for all of the ports included in the FSN. The MTU size can be set to a custom value between 1280 and 9216. Specific I/O modules may restrict allowed range for MTU size value. The MTU size values of 1500 bytes (default) and 9000 bytes (jumbo frame) are supported by all interfaces and I/O modules.

Example 1

The following example changes the MTU size of the FSN "spa_fsn_0".

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/fsn -d
spa_fsn_0 set -mtuSize 9000
```

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

ID = spa_fsn_0
ID = spb_fsn_0
```

```
Operation completed successfully.
```

Example 2
The following example shows an attempt to add Ethernet port "spa_iom_0_eth2" to FSN "spa_fsn_0", however this ethernet port is already in use for another link aggregation and could not be added independently to the FSN.

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/fsn -d spa_fsn_0 set -secondaryPorts spa_iom_0_eth2`

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

Operation failed. Error code: 0x6000851
One of the specified ports cannot be used to configure an FSN
because to it is already included in an FSN or link aggregation.
(Error Code:0x6000851)
```

Delete an FSN

Delete an FSN from the system.

Delete a fail-safe network.

Format
`/net/fsn -id <value> delete`

Object qualifier

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

Example
The following example deletes FSN "spa_fsn_0"

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/fsn -id spa_fsn_0 delete`

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

ID = spa_fsn_0
ID = spb_fsn_0

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 host names 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 domains allow configuring DNS server addresses. All addresses are grouped under user-defined DNS server domains. DNS settings are identified by NAS server domain ID. NAS server DNS settings should allow DNS resolution of all names within an SMB server domain in order for the SMB protocol to operate normally within an Active Directory domain.

NOTICE

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 57 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.
`Replication sync`	Indicates the status of the DNS list in the NAS server operating as a replication destination. When a replicated DNS servers list is created on the source NAS server, it is automatically synchronized to the destination. Valid values are: • `Not replicated` – DNS list is not replicated over to the destination. • `Auto synchronized` – DNS list is automatically synchronized over to the replication destination. Any modify or delete operations at the source will automatically be reflected on the destination. • `Overridden` – DNS list has been manually modified or overridden on the replication destination. Modifications or deletions of addresses from the DNS list on the source NAS server will have no effect on the overridden DNS list on the replication destination.

Table 57 DNS domain and server attributes (continued)

Attribute	Description
	Note When a DNS list is disabled or deleted from the source, overridden DNS list in the destination may not get disabled or deleted automatically.
`Source name servers`	List of name server IP addresses defined on the replication source.

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.

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

The show action command on page 23 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 -detail
```

```
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
       Replication sync    = Overridden
       Source 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} [-replSync {auto | overridden}]
```

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.
`-replSync`	Status of the DNS list in the NAS server operating as a replication destination. Valid values are: • `auto` • `overridden`

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 (SMB) 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 58 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

The show action command on page 23 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 59 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.
`Replication sync`	Indicates the status of the NIS server addresses list in the NAS server operating as a replication destination. When a replicated NIS servers list is created on the source NAS

Table 59 NIS server domain attributes (continued)

Attribute	Description
	server, it is automatically synchronized to the destination. Valid values are: • `Not replicated` – NIS list is not replicated over to the destination. • `Auto synchronized` – NIS list is automatically synchronized over to the replication destination. Any modify or delete operations at the source will automatically be reflected on the destination. • `Overridden` – NIS list has been manually modified or overridden on the replication destination. Modifications or deletions of addresses from the NIS list on the source NAS server will have no effect on the overridden NIS list on the replication destination. **Note** When a NIS list is disabled or deleted from the source, overridden NIS list in the destination may not get disabled or deleted automatically.
`Source servers`	List of IP addresses for the NIS servers defined on the replication source.

View NIS server domains

View details about NIS server domains.

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 -detail
```

```
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
        Replication sync = Overridden
        Source servers   = 10.64.74.74,10.64.74.1
```

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}} [-replSync {auto | overridden}]
```

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.
`-replSync`	Status of the NIS list in the NAS server operating as a replication destination. Valid values are: • `auto` • `overridden`

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. 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.

Configure alert settings on page 643 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 60 SMTP server attributes

Attribute	Description
`ID`	ID of the SMTP server.
`Address`	IP address of the SMTP server.
`Port`	Port of the SMTP server.
`Encryption level`	Encryption level (SSL method) used to communicate with the SMTP server. Valid values are: • None • Start TLS • SSL
`Authentication type`	Type of authentication used to log in to the SMTP server. Valid value are: • None • Plain • Login • CRAM_MD5 • DIGEST_MD5
`User name`	User name used to log in to the SMTP server.
`Bypass proxy`	Indicates whether or not the global proxy settings will be bypassed. • `yes`: Global proxy server settings are ignored and the SMTP server will be accessed directly. • `no` (default): Global proxy server settings are used to access the SMTP server.

View SMTP server settings

View the IP addresses of the SMTP servers.

Note

The show action command on page 23 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
       Port                = 25
       Encryption level    = SSL
       Authentication type = Plain
       User name           = test
       Bypass proxy        = no
```

Configure SMTP server settings

Specify the IP addresses for the SMTP server setting.

Format

```
/net/smtp -id <value> set -addr <value> [-port <value>] [-encryptLevel {none|startTLS|ssl}] [-authType {none|plain|login|cram_md5|digest_md5}] [-user <value> {-passwd <value> |-passwdSecure}][-bypassproxy {yes|no}]
```

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.
`-port`	Enter the port of the SMTP server.
`-encryptLevel`	Specifies the encryption level (SSL method) of the SMTP server. Valid values are: • `none` • `startTLS` • `ssl`
`-authType`	Specifies the authentication type of the SMTP server. Valid values are:

Qualifier	Description
	• none • plain • login • cram_md5 • digest_md5
-user	Specifies the user name of the SMTP server.
-passwd	Specifies the password of the SMTP server.
-passwdSecure	Specifies the password in secure mode. The user will be prompted to input the password.
-bypassproxy	Specifies whether the global proxy settings are bypassed when accessing the SMTP server. Valid values are: • yes: Ignores the global proxy server settings to access the SMTP server directly. • no (default): Uses the global proxy server settings.

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 -port 25 -encryptLevel ssl -authType
plain -user test -passwd test
```

```
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 61 NDMP server attributes

Attribute	Description
NAS server	ID of the associated NAS server.

Table 61 NDMP server attributes (continued)

Attribute	Description
`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.

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.

Note

If you intend to use LDAP with SSL, you must upload the CA certificate of the LDAP server to the system by using the `-upload` command before configuring the LDAP settings. For example:

```
uemcli -d 10.0.0.1 -u admin -p MyPwd -upload -f /tmp/
myldapservercertificate.cer
/sys/cert -type CA -service Mgmt_LDAP
```

Table 62 LDAP server attributes

Attribute	Description
`ID`	ID of the LDAP server.
`Auto discovery enabled`	Indicates whether the LDAP server names are obtained using DNS. To use this feature, the DNS server for the LDAP domain must be configured as the first server in the list of DNS servers.
`Name`	Server hostnames or IP addresses of the LDAP servers, specified as a comma-separated list. If IP addresses are specified, the DNS Server for the LDAP domain must be configured with a reverse lookup so that it provides the FQDN for the specified IP addresses.
`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 SSL (LDAPS) uses port 636. For forest-level authentication, specify port 3268 for LDAP or port 3269 for LDAPS.
`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.
`Bind DN`	Distinguished name (DN) for a user with administrator privileges on the LDAP Server. The DN can be expressed in several formats. For example: **`cn=Administrator,cn=Users,dc=mycompany,dc=com`** **`Administrator@mycompany.com`** **`mycompany.com/Administrator`**
`Bind password`	Password to be used for binding to the LDAP server. This is the password for the user specified in the `Bind DN` attribute.
`User search path`	Path to search for users on the directory server. For example: ou=People,dc=lss,dc=emc,dc=com.

Table 62 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. For forest-level authenticaion, specify **`userPrincipalName`**.
`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 (filename of) the trusted certificate file used for one-way LDAP server authentication. The chain cannot contain the server certificate.
`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.

Note

If you intend to use LDAP with SSL, you must upload the CA certificate of the LDAP server to the system by using the `-upload` command before configuring the LDAP settings. For example:

```
uemcli -d 10.0.0.1 -u admin -p MyPwd -upload -f /tmp/
myldapservercertificate.cer
/sys/cert -type CA -service Mgmt_LDAP
```

Format

```
/net/ldap create [{-name <value> | -autoDiscoveryEnabled}] –
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 LDAP IP addresses or hostnames as a comma-separated string. If IP addresses are specified, the DNS server for the LDAP domain must be configured with a reverse lookup so that it provides the FQDN for a specified IP address.
`-autoDiscoveryEnabled`	Specify to direct the system to obtain the LDAP server addresses using DNS. To use this feature, the DNS server for the LDAP domain must be configured as the first server in the list of DNS servers. **Note** `-autoDiscoveryEnabled` is the default if you do not specify either `-name` or `-autoDiscoveryEnabled`.
`-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. Valid values are: • `ldap` (default) — LDAP without SSL. • `ldaps` — LDAP with SSL.
`-certFilePath`	Path to (filename of) the trusted certificate file used for one way server authentication.

Qualifier	Description
	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. For forest-level authentication, specify port 3268 for LDAP or port 3269 for LDAPS.

`-bindDn`	Type the distinguished name (DN) for a user with administrator privileges on the LDAP Server. The DN can be expressed in several formats. For example:
	`cn=Administrator,cn=Users,dc=mycompany,dc=com`
	`Administrator@mycompany.com`
	`mycompany.com/Administrator`

`-bindPasswd`	Type the password to be used for binding to the LDAP server. This is the password for the user specified in the `Bind DN` attribute.
`-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>. **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.

Qualifier	Description
`-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 1: Creating an LDAP configuration with a specific LDAP server address specified

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/ldap create -
name lpso242.lss.emc.com -domain domain.example.com -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: 10.64.75.201
Storage system port: 443
HTTPS connection

ID = LDAP_1
Operation completed successfully.
```

Example 2: Creating an LDAP configuration with multiple LDAP server address specified

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/ldap create -
name lpso242.lss.emc.com,lpso243.lss.emc.com -domain
domain.example.com -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: 10.64.75.201
Storage system port: 443
HTTPS connection

ID = LDAP_1
Operation completed successfully
```

Example 3: Creating an LDAP configuration using auto discovery through DNS to configure the server addresses

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/ldap create -
autoDiscoveryEnabled -domain domain.example.com -port 389 -protocol
ldap -bindDn "cn=Administartor,ou=Users,dc=domain,dc=example,dc=com" -
bindPasswd Password0123 -userSearchPath
"ou=Users,dc=domain,dc=example,dc=com" -groupSearchPath
"ou=Groups,dc=domain,dc=example,dc=com" -userIdAttr "uid" -
```

```
groupNameAttr "cn" -userObjectClass "interOrgPerson" -groupObjectClass
"groupOfUniqueNames" -groupMemberAttr "uniqueMember" -timeout 40000
```

```
Storage system address: 10.64.75.201
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 23 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.

Note

If you intend to use LDAP with SSL, you must upload the CA certificate of the LDAP server to the system by using the `-upload` command before configuring the LDAP settings. For example:

```
uemcli -d 10.0.0.1 -u admin -p MyPwd -upload -f /tmp/
myldapservercertificate.cer
/sys/cert -type CA -service Mgmt_LDAP
```

Format

```
/net/ldap -id <value> set [{-name <value> | -autoDiscoveryEnabled}] [-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 IP addresses or hostnames of the primary directory servers to use for authentication. The values you type depends on the format of the subject field entry in each directory server's certificate. Typically, this requires a hostname. Type the LDAP IP addresses or hostnames as a comma-separated string. If IP addresses are specified, the DNS Server for the LDAP domain must be configured with a reverse lookup so that it provides the FQDN for the specified IP addresses.
`-autoDiscoveryEnabled`	Specify to direct the system to obtain the LDAP server addresses or hostnames using DNS. DNS must be configured for this option to take effect. **Note** `-autoDiscoveryEnabled` is the default if you do not specify either `-name` or `-autoDiscoveryEnabled`.
`-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. For forest-level authentication, specify port 3268 for LDAP or port 3269 for LDAPS.
`-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.

Qualifier	Description
`-certFilePath`	Path to (filename of) the trusted certificate file used for one way server authentication. **Note** If the value of `-protocol` is `ldaps`, this qualifier is required.

`-bindDn`	Type the distinguished name (DN) for a user with administrator privileges on the LDAP Server. The DN can be expressed in several formats. For example:
	`cn=Administrator,cn=Users,dc=mycompany,dc=com`
	`Administrator@mycompany.com`
	`mycompany.com/Administrator`

`-bindPasswd`	Type the password to be used for binding to the LDAP server. This is the password for the user specified in the `Bind DN` attribute. It 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

Qualifier	Description
	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.
```

Refresh the automatically-discovered LDAP server address list

Refreshes the auto discovered server address list for the specified LDAP server configuration. This can only be performed if auto-discovery is enabled.

Format
`/net/ldap -id <value> refresh`

Object qualifier

Qualifier	Description
`-id`	Identifies the LDAP server.

Example

The following command refreshes the automatically-discovered LDAP server address list for the LDAP_1 server configuration:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/ldap -id LDAP_1
refresh
```

```
Storage system address: 10.64.75.201
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 NAS server interface (`-srcIf` parameter value).

Format

```
/net/util ping -srcIf <value> -addr <value>
```

Action qualifier

Qualifier	Description
`-srcIf`	Identifies the NAS server interface from which the packet will be sent. The value is an interface identifier. Use this qualifier when you want to test whether a specific NAS server interface can access a remote host.
`-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 10.0.0.1
```

```
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 is an interface identifier.
`-addr`	Specify the destination address to use when sending the packet.

Example

The following example shows trace route to a remote host:

```
uemcli /net/util/traceroute -srcIf if_0 -addr 10.0.0.1
```

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

1: Result = traceroute to 10.0.0.1 (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 Distributed Hierarchical Storage Management

Distributed Hierarchical Storage Management (DHSM) is required by the vCenter Plug-in application. The DHSM feature allows the VCenter Plug-in user to perform advanced file system functions.

Note

This feature was formerly called Advanced Storage Access (ASA).

The following table lists the attributes for DHSM.

Table 63 DHSM attributes

Attribute	Description
`NAS server`	NAS server ID.
`State`	The state of the DHSM service. Valid values are: • `disabled` • `enabled`
`Username`	The DHSM user name.
`Password`	The DHSM user password.
`HTTPS enabled`	Specifies whether SSL (HTTPS) is required for DHSM requests to this DHSM server. Valid values are: • `yes` (default) • `no`

View DHSM settings

Displays DHSM settings.

Format

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

Object qualifier

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

Example

The following command displays the DHSM settings:

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

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

1:     NAS server    = nas_0
       State         = Enabled
       Username      = Local/joe
       HTTPS enabled = no
```

Change Distributed Hierarchical Storage Management settings

Modifies the Distributed Hierarchical Storage Management (DHSM) settings.

Format

```
/net/nas/dhsm -server <value> set [-state {Disabled | Enabled}]
[[-username <value>] {-passwd <value> | -passwdSecure}] [-
enableHTTPS {yes|no}]
```

Object qualifier

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

Action qualifier

Qualifier	Description
`-state`	Specifies whether the DHSM service is enabled. Possible values include: • `Disabled` — DHSM service is disabled. • `Enabled` — DHSM service is enabled.
`-username`	Specifies the DHSM user name.
`-passwd`	Specifies the DHSM user password. **Note** This attribute is mandatory if the current state is being changed from Disabled to EnabledPerHost or EnabledForAll.
`-passwdSecure`	Specifies the password in secure mode. The user is prompted to specify the password and confirm the password.
`-enableHTTPS`	Specifies whether SSL (HTTPS) is required for DHSM requests to this DHSM server. Valid values are: • `yes` • `no`

Example

The following command changes the DHSM password:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/dhsm –
server nas_0 set –state Enabled –username newname –passwd newpassword
```

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

Operation completed successfully.
```

Manage DHSM Connection

Distributed Hierarchical Storage Management (DHSM) connection is required for the Cloud Tiering Appliance (CTA) integration with Unity. The DHSM connection feature allows Unity file system data to be archived to CTA and recalled from CTA.

The following table lists the attributes for DHSM connection.

Table 64 DHSM connection attributes

Attribute	Description
`ID`	DHSM connection identifier.
`Secondary URL`	Specifies the protocol (HTTP) and the host name of the secondary storage server. It optionally specifies a portion of the hierarchical namespace published by the web server. While both an IP address and fully qualified domain name (FQDN) are allowed to specify as the host name, it is recommended to use FQDN.
`Secondary port`	Port of the secondary storage server.
`Local port`	Local port of the DHSM connections.
`Secondary username`	Username that the storage array uses if HTTP digest authentication is required by the secondary storage.
`Timeout`	Timeout in seconds when the connection is established to the secondary storage. If recall does not return within the timeout period specified, the NAS server tries another DHSM connection. Default value is 30 seconds.
`File system`	File system storage resource on which the connection is created.
`Mode`	Mode of the connection. Valid values are: • `Disabled` – cannot create stub files or migrate data. Data currently on the NAS server can be read and written to. • `Enabled` (default) – allows both the creation of stub files and data migration through reads and writes. • `Recall only` – the policy engine is not allowed to create stub files, but the user is still able to trigger data migration by using a read or write request from the secondary file system to Unity.
`Read policy`	Read policy when the NAS server recalls data from the secondary storage. • `Full` – recalls the whole file to the NAS server on a read request before the data is returned.

Table 64 DHSM connection attributes (continued)

Attribute	Description
	- `Passthrough` – retrieves data without recalling the data to Unity. - `Partial` – recalls only the data blocks required to satisfy the client read request. - `None` – uses the read method option specified in the stub file.

Create a DHSM connection

Create a DHSM connection by using the HTTP protocol between the specified primary file system of Unity and a secondary file system of CTA.

Format

```
/net/nas/dhsmconn create [-async] -fs <value> -secondaryUrl
<value> [-secondaryPort <value>] [-localPort <value>] [-mode
{enabled | disabled | recallOnly}] [-readPolicy {none | full |
passthrough | partial}] [-secondaryUsername <value>] [-
secondaryPassword <value>] [-timeout <value>]
```

Action qualifiers

Qualifier	Description
`-fs`	Specifies the file system storage resource ID.
`-secondaryUrl`	Specifies the URL of the remote secondary storage, including the protocol, the host name and optionally a portion of the published hierarchical namespace.
`-secondaryPort`	Specifies the remote port number that the nas server delivers the HTTP request to. If not specified, the Data Mover issues HTTP requests to port 80 on the secondary storage HTTP server.
`-localPort`	Specifies the local port of the DHSM connection.
`-mode`	Sets the mode of Unity DHSM operations on the specified file system. Valid values are: - `enabled` (default) – allows both the creation of stub files and data migration through reads and writes - `disabled` – neither stub files nor data migration is possible. Data currently on the Unity can be read and written to in the disabled mode. - `recallOnly` – the policy engine is not allowed to create stub files, but the user is still able to trigger data migration using a read or write request from the secondary file system to the Unity.
`-readPolicy`	Specifies the migration method option used by the Unity in the connection level, to override the migration method specified in the stub file. Valid values are:

Qualifier	Description
	• `none` (default) – specifies no override. • `full` – recalls the whole file to Unity on a read request before the data is returned. • `passthrough` – retrieves data without recalling the data to Unity. • `partial` – recalls only the blocks required to satisfy the client read request.
`-secondaryUsername`	Defines the username the HTTP client uses if digest authentication is required by the secondary storage HTTP server.
`-secondaryPassword`	Specifies the password associated with the username required by the secondary storage server.
`-timeout`	Specifies the timeout value in seconds. By default, the Unity HTTP client waits 30 seconds for a reply from the HTTP server and then retries the operation once.

Example

The following command creates an HTTP connection for file system "fs_1" to the secondary file system /export/dhsm1 on http://10.1.0.115.

```
uemcli /net/nas/dhsmconn create -filesystem fs_1 -secondaryUrl http://
10.1.0.115/export/dhsm1
```

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

ID = dhsmconn_1
Operation completed successfully.
```

View DHSM connection settings

View details for DHSM connections.

Format

`/net/nas/dhsmconn [{-id <value> | -fs <value>}] show`

Action qualifiers

Qualifier	Description
`-id`	DHSM connection identifier.
`-fs`	Specifies the file system storage resource ID.

Example 1

The following command shows all DHSM connections for file system "fs_1".

```
uemcli /net/nas/dhsmconn –fs fs_1 show
```

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

```
HTTPS connection

1:  ID                 = dhsmconn_0
    File system        = fs_1
    Mode               = enabled
    Read policy        = none
    Secondary url      = http://172.24.102.115/export/dhsm1
    Secondary port     = 80
    Secondary username = admin
    Local port         = 80
    Timeout            = 60
```

Example 2

The following command shows DHSM connection "dhsmconn_1".

uemcli /net/nas/dhsmconn –id dhsmconn_1 show

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

1:  ID                 = dhsmconn_1
    File system        = fs_1
    Mode               = disabled
    Read policy        = full
    Secondary url      = http://www.myserver.com/export/dhsm1
    Secondary port     = 80
    Secondary username = admin
    Local port         = 80
    Timeout            = 60
```

Example 3

The following command shows all DHSM connections on the storage system.

uemcli /net/nas/dhsmconn show

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

1:  ID                 = dhsmconn_0
    File system        = fs_1
    Mode               = enabled
    Read policy        = none
    Secondary url      = http://10.1.0.115/export/dhsm1
    Secondary port     = 80
    Secondary username = admin
    Local port         = 80
    Timeout            = 60

2:  ID                 = dhsmconn_1
    File system        = fs_2
    Mode               = disabled
    Read policy        = full
    Secondary url      = http://10.1.0.115/export/dhsm1
    Secondary port     = 80
    Secondary username = admin
    Local port         = 80
    Timeout            = 60

3:  ID                 = dhsmconn_2
    File system        = fs_3
    Mode               = enabled
```

```
     Read policy         = passthrough
     Secondary url       = http://10.1.0.115/export/dhsm2
     Secondary port      = 80
     Secondary username  = admin
     Local port          = 80
     Timeout             = 60
```

Change DHSM connection settings

Modify settings for an existing DHSM connection.

Format

`/net/nas/dhsmconn –id <value> modify [-async] [-mode {enabled | disabled | recallOnly}] [-readPolicy {full | passthrough | partial | none}] [-secondaryServerName <value> [-secondaryPort <value>] [-localPort <value>] [-secondaryUsername <value> -secondaryPassword <value>] [-timeout <value>]`

Action qualifiers

Qualifier	Description
-id	DHSM connection identifier.
-mode	Sets the mode of Unity DHSM operations on the specified file system. Valid values are: • `enabled` (default) – allows both the creation of stub files and data migration through reads and writes • `disabled` – neither stub files nor data migration is possible. Data currently on the Unity can be read and written to in the disabled mode. • `recallOnly` – the policy engine is not allowed to create stub files, but the user is still able to trigger data migration using a read or write request from the secondary file system to the Unity.
-readPolicy	Specifies the migration method option used by the Unity in the connection level, to override the migration method specified in the stub file. Valid values are: • `none` (default) – specifies no override. • `full` – recalls the whole file to Unity on a read request before the data is returned. • `passthrough` – retrieves data without recalling the data to Unity. • `partial` – recalls only the blocks required to satisfy the client read request.
-secondaryServerName	Specifies the remote server name or IP address.
-secondaryPort	Specifies the remote port number that the NAS server delivers the HTTP request to. If not specified, the NAS server issues HTTP requests to port 80 on the secondary storage HTTP server.

Qualifier	Description
-secondaryUsername	Defines the username the HTTP client uses if digest authentication is required by the secondary storage HTTP server.
-secondaryPassword	Specifies the password associated with the username required by the secondary storage server.
-timeout	Specifies the timeout value in seconds. By default, the Unity HTTP client waits 30 seconds for a reply from the HTTP server and then retries the operation once.

Example 1

The following command modifies the mode of connection "dhsmconn_1".

```
uemcli /net/nas/dhsmconn –id dhsmconn_1 modify -mode recallOnly
```

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

ID = dhsmconn_1
Operation completed successfully.
```

Example 2

The following command modifies the readPolicy setting for connection "dhsmconn_1".

```
uemcli /net/nas/dhsmconn –id dhsmconn_1 modify –readPolicy passthrough
```

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

ID = dhsmconn_1
Operation completed successfully.
```

Delete a DHSM connection

Deletes an existing HTTP connection between the file system and the secondary file system.

Format

```
/net/nas/dhsmconn -id <value> delete [-async] [-recallPolicyOnDelete {fail | no | yes}]
```

Action qualifiers

Qualifier	Description
-id	DHSM connection identifier.
-recallPolicyOnDelete	Specifies the recall policy for any migrated file during the delete operation. Valid values are: • fail (default) – scans the file system for stub files that depend on the connection and fails on the first one.

Qualifier	Description
	• `no` – deletes the connection without checking for stub files that depend on the connection. If the `no` option is specified and stub files exist, an I/O error appears when the file is read because the connection no longer exists. • `yes` – migrates the files back to Unity before the connection is deleted.

Example

The following command deletes the DHSM connection "dhsmconn_1" and specifies the recall policy for any migrated files during the delete operation.

```
uemcli /net/nas/dhsmconn -id dhsmconn_1 delete -recallPolicy no
```

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

Operation completed successfully.
```

Manage the tie breaker node (dual-SP virtual deployments only)

Using a Tie Breaker Node (TBN) can increase the availability of your storage system. To enable a TBN, see Change tie breaker node configuration settings on page 269

Table 65 TBN configuration attributes

Attribute	Description
`ID`	TBN identifier.
`Health state`	Health state of the TBN. The health state code appears in parentheses. Value is one of the following: • `Unknown (0)`—The health of the TBN cannot be determined. • `OK (5)`—TBN is operating normally. • `Degraded/Warning (10)`—TBN service is working, but one or more of the following may have occurred: ▪ TBN can communicate with SPA through one network heartbeat link, but not both. One network heartbeat link between them is disconnected. ▪ TBN can communicate with SPB through one network heartbeat link, but not both. One network heartbeat link between them is disconnected.

Table 65 TBN configuration attributes (continued)

Attribute	Description
	▪ TBN can communicate with each SP through one network heartbeat link separately, but through not both heartbeat links. One network heartbeat link between the TBN and SPA is disconnected. One heartbeat link between the TBN and SPB is also disconnected. • `Minor failure (15)`—One or of the following occurred: ▪ TBN is disconnected from SPA. Both network heartbeat links between the TBN and SPA are disconnected. ▪ TBN is disconnected from SPB. Both network heartbeat links between the TBN and SPB are disconnected. • `Major failure (20)`—TBN is disconnected from SPA and SPB. All network heartbeat links between the TBN and SPA, and the TBN and SPB are disconnected.
`Health details`	Additional health information. See Appendix A, Reference, for health information details.
`Active`	Indicates whether the TBN service is active. Valid values are: • `yes` • `no`

View basic tie breaker node information

Display basic Tie Breaker Node (TBN) information, including the TBN identifier and health state for an active TBN.

Format

`/net/tbn [-id <value>] show`

Example 1 Example

The following command shows basic TBN information:

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

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

1:     ID                                  =
```

Example 1 Example (continued)

```
42389FCA-01D1-4491-7D77-8060373D67B8
       Health state                             = OK (5)
       Active                                   = yes
```

Manage a tie breaker node configuration (dual-SP virtual deployments only)

A Tie Breaker Node (TBN) enables a dual-SP UnityVSA to prevent data corruption resulting from a "split-brain" situation, which occurs when the two SPs stop communicating and synchronizing their data with each other. Enabling a TBN prevents this situation and can increase the availability of your storage system.

Table 66 TBN configuration attributes

Attribute	Description
`Enabled`	Indicates whether the TBN is enabled. Valid values are: • `yes` • `no`
`Active TBN`	TBN identifier.

View tie breaker node configuration settings

View details about Tie Breaker Node (TBN) configuration settings.

Format

`/net/tbn/config show`

Example 2 Example

The following command shows details for the TBN configuration:

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

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

1:     Enabled                                  = yes
       Active TBN                               =
42389FCA-01D1-4491-7D77-8060373D67B8
```

Change tie breaker node configuration settings

Modify the Tie Breaker Node (TBN) configuration.

Format

```
/net/tbn/config set [-enabled {yes|no}] [-activeTbn <value>]
```

Action qualifier

Qualifier	Description
`-enabled`	Enable or disable a TBN. Valid values are: • yes • no
`-activeTbn`	Specify the TBN identifier: • Use this value with the `-enabled` qualifier to enable the specified TBN. • Use this value without the `-enabled` qualifier to activate the specified TBN. The TBN identifier is not needed when the value of the `-enabled` qualifier is no.

Example 1: Enable a TBN

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/tbn/config set -enabled yes -activeTbn 42389FCA-01D1-4491-7D77-8060373D67B8`

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

Operation completed successfully.
```

Example 2: Disable a TBN

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/tbn/config set -enabled no`

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

Operation completed successfully
```

Example 3: Change the active TBN

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/tbn/config set -activeTbn 42389FCA-01D1-4491-7D77-8060373D67B8`

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

Operation completed successfully
```

CHAPTER 4

Manage Hosts

This chapter contains 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.

Each host configuration is identified by an ID.

The following table lists the attributes for host configurations.

Table 67 Host configuration attributes

Attribute	Description
`ID`	ID of the host configuration.
`Name`	Name of the host configuration.
`Description`	Brief description of the host configuration.
`Tenant`	Tenant with which the host is associated.
`Address`	Hostname or IP address associated with the host, IP address of the subnet, or name 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` — 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 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.

Table 67 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 240 explains how to configure NIS server communication.
`OS type`	Type of operating system (OS) running on the host. You can enter any value you want. Here are suggestions for some of the common operating systems: • `undefined` — OS is not specified (default) or unknown. • `other` — Other. • `win2003srv` — Windows Server 2003. • `winxp` — Windows XP. • `win2008srv` — Windows Server 2008. • `winvista` — Windows Vista. • `win2012srv` — Windows Server 2012. • `esx` — VMware ESX. • `redhat` — Red Hat Enterprise Linux. • `sles` — SUSE Linux Enterprise. • `win7` — Windows 7. • `hyperv` — Microsoft Hyper-V. • `solaris` — Solaris.
`Ignored address`	A comma-separated list of host IP addresses to exclude from data access.
`Health state`	Health state of the host. 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 67 Host configuration attributes (continued)

Attribute	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.
`Management type`	Indicates the way the host is managed. Value is one of the following: - `VMware` — The host is managed through VMware web services. - `Other` — The host is automatically created on the storage system. - `Manual` — The host is created manually.
`Accessible LUNs`	A comma-separate list of LUNs that are accessible to the host.
`Host LUN IDs`	Comma-separated list of HLUs (Host LUN identifiers), which the corresponding hosts use to access the LUN.

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>] [-tenant
<value>] -type {host [-addr <value>] [-ignoredAddr <value>] [-
osType <value> ] | 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.
`-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 addresses. A subnet mask, or network mask, defines the boundaries of an IP subnet.

Qualifier	Description
	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 240 explains how to configure NIS server communication.
`-tenant`	Specifies the identifier of the tenant with which the host is to be associated. **Note** If not specified, the host is created in the default network namespace and the tenant attribute will be blank.
`-addr`	Specifies the hostnames or IP addresses associated with the host, IP addresses of the subnet, or the name of the netgroup. Separate each value with a comma. • Format: *<IP address>*/[*<prefix length>*]. • Default prefix length for IPv4 addresses is 24 and for IPv6 addresses 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 for the host configuration.
`-osType`	Specify the type of operating system (OS) running on the host. You can enter any value you want. Here are suggestions for some of the common operating systems: • `undefined` — OS is not specified (default) or unknown. • `other` — Other. • `win2003srv` — Windows Server 2003. • `winxp` — Windows XP. • `win2008srv` — Windows Server 2008. • `winvista` — Windows Vista.

Qualifier	Description
	• `win2012srv` — Windows Server 2012. • `esx` — VMware ESX. • `redhat` — Red Hat Enterprise Linux. • `sles` — SUSE Linux Enterprise. • `win7` — Windows 7. • `hyperv` — Microsoft Hyper-V. • `solaris` — Solaris.

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 Host_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 = Host_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 Subnet_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 = Subnet_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 NetGroup_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 = NetGroup_1023
Operation completed successfully.
```

View host configurations

View details about a host configuration. You can select the ID of the host configuration or the host type.

Note

The show action command on page 23 explains how to change the output format.

Format

```
/remote/host [{{-id <value> | -name <value>} | -type {host |
subnet | netgroup}}] show
```

Object qualifier

Qualifier	Description
-id	Specify the host ID.
-name	Specify the host name.
-type	Specifies the host type. Valid values are: • host • subnet • 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 -
brief
```

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

1:      ID               = 1014
```

```
        Name            = MyHost
        Description     = this is my host
        Tenant          = tenant_3
        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
        Tenant          =
        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> | -name <value>} set [-name <value>]
[-descr <value>] [-addr <value>] [-ignoredAddr <value>] [-
netmask <value>] [-osType <value>] [-addLuns <value> [-hlus
<value> ]] [-removeLuns <value>]
```

Object qualifier

Qualifier	Description
-id	ID of the host configuration to change.
-name	Name of 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 name. • Format: *<IP address>/*[*<prefix length>*]. • Default prefix length for IPv4 addresses is 24 and for IPv6 addresses is 64.

Qualifier	Description
	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`	Specify the subnet mask for the host configuration.
`-osType`	Specify the type of operating system (OS) running on the host. You can enter any value you want. Here are suggestions for some of the common operating systems: • `undefined` — OS is not specified or unknown. • `other` — Other. • `win2003srv` — Windows Server 2003. • `winxp` — Windows XP. • `win2008srv` — Windows Server 2008. • `winvista` — Windows Vista. • `win2012srv` — Windows Server 2012. • `esx` — VMware ESX. • `redhat` — Red Hat Enterprise Linux. • `sles` — SUSE Linux Enterprise. • `win7` — Windows 7. • `hyperv` — Microsoft Hyper-V. • `solaris` — Solaris.
`-addLuns`	Specify a comma-separated list of LUN friendly IDs for LUNs to add to the host.
`-hlus`	Specifies the comma-separated list of Host LUN identifiers to be used by the corresponding hosts which were specified in the `–lunHosts` option. The number of items in the two lists must match. However, an empty string is a valid value for any element of the Host LUN identifiers list, as long as commas separate the list elements. Such an empty element signifies that the system should automatically assign the Host LUN identifier value by which the corresponding host will access the LUN. If not specified, the system will automatically assign the Host LUN identifier value for every host specified in the `-lunHosts` argument list.
`-removeLuns`	Specify a comma-separated list of LUN friendly IDs for LUNs to remove from the host.

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.

NOTICE

Deleting a host configuration breaks the block-based (Fibre Channel or iSCSI) 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> | -name <value>} delete
```

Object qualifier

Qualifier	Description
-id	ID of the host configuration to delete.
-name	Name of 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 and read/write snapshots of a production LUN.

Each host LUN is identified by an ID.

The following table lists the attributes for host LUNs.

Table 68 Host LUN attributes

Attribute	Description
`ID`	Unique identifier of the host LUN (HLU).
`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 name`	LUN name.
`Snapshot`	Snapshot ID of a LUN or consistency group.
`Snapshot name`	Snapshot name of a LUN or consistency group.
`LUN ID`	Logical unit number on the host, or the host LUN ID.
`Access`	Access permission for the host. Valid values are: • `read-only` • `read/write`
`LUN type`	LUN type. Valid values are: • `snap` • `production`

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 23 explains how to change the output format.

Format

```
/remote/host/hlu { -id <value> | -host <value> | -hostName
<value> | -lun <value> | -lunName <value> | { -host <value> | -
hostName <value> } { -lun <value> | -lunName <value> } } [-type
{ production | snap } ] show
```

Object qualifier

Qualifier	Description
`-id`	Specifies the host LUN ID.
`-host`	Specifies the host ID.
`-hostName`	Specifies the host name.
`-lun`	Specifies the LUN ID.
`-lunName`	Specifies the LUN name.
`-type`	Specifies the LUN type.

Example

The following command lists all host LUNs on host Host_3:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/host/hlu -host Host_3 show -detail`

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

1:     ID             = Host_3_sv_2_prod
       Host           = Host_3
       Host name      = 10.0.0.2
       LUN            = sv_2
       LUN name       = joeslun
       Snapshot       =
       Snapshot name  =
       LUN ID         = 1
       Access         = Read/write
       LUN type       = Production
```

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 {-id <value>} set -lunid <value>`

Object qualifier

Qualifier	Description
`-id`	Specifies the HLU.

Action qualifier

Qualifier	Description
`-lunid`	Specifies the new LUN ID for the LUN on the selected host.

Example

The following command changes the ID Host_3_sv_2_prod to LUN 0:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/host/hlu -id Host_3_sv_2_prod 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 one or more initiators for each host configuration that accesses the storage system. Each 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.

A FC initiator contains the WWN of an HBA on the host. This WWN is not the WWN of the host.

An iSCSI initiator contains the IQN (iSCSI Qualified Name) used by the host, and optionally the CHAP authentication password associated with the host. Manage reverse CHAP for mutual CHAP authentication on page 194 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 69 Initiator attributes

Attribute	Description
`ID`	Host initiator ID.
`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.

Table 69 Initiator attributes (continued)

Attribute	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.
`CHAP users`	List of CHAP accounts configured for the initiator.
`Source type`	The source initiator type. Values are: • `HPAutotrespass` - HP with Auto-trespass • `OpenNative` (default) - Open native (such as CLARiiON Open) • `SGI` - Silicon Graphics • `HPNoAutotrespass`- HP without Auto-trespass • `Dell` • `FujitsuSiemens` • `Tru64`- Compaq Tru64
`Failover mode`	The failover mode for the initiator. Values are: • `AutoTrespass`- Any media access to the non owning SP is rejected. • `PassiveNotReady`- A command failure during I/O is sent to the non-owning SP. • `DMP`- Quiet trespass on I/O to non owning SP. • `PassiveAlwaysReady`- Some commands, e.g. Test Unit Ready, returns PAR status. • `ALUA`(default) - Initiators are permitted to send I/O to a LUN regardless of which SP actually owns the LUN.
`LUNZ enabled`	Specifies whether LUNZ is enabled. Values are: • `yes` • `no`
`Unit serial number`	Indicates the unity serial number. Values are: • `Array` (default) • `LUN` For SCSI-3 interfaces, the Unity Serial Number page (Vital Product Data page 0x80) reports the serial number for the array or LUN.

Create 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} [-sourceType {HPAutotrespass | OpenNative | SGI |
HPNoAutotrespass | Dell | FujitsuSiemens | Tru64}] [-
failoverMode {AutoTrespass | PassiveNotReady | DMP |
PassiveAlwaysReady | ALUA}] [-lunzEnabled {yes | no}] [-
unitSerialNumber {Array | LUN}]
```

Object qualifier

Qualifier	Description
`-host`	Identifies the host configuration to which to assign the initiator. View host configurations on page 277 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`
`-sourceType`	Specify the source type for the initiator. Valid values are: • `HPAutotrespass` - HP with Auto-trespass • `OpenNative` (default) - Open native (such as CLARiiON Open) • `SGI` - Silicon Graphics • `HPNoAutotrespass`- HP without Auto-trespass • `Dell` • `FujitsuSiemens` • `Tru64`- Compaq Tru64
`-failoverMode`	Specify the failover mode for the initiator. Valid values are: • `AutoTrespass`- Any media access to the non owning SP is rejected. • `PassiveNotReady`- A command failure during I/O is sent to the non-owning SP. • `DMP`- Quiet trespass on I/O to non owning SP. • `PassiveAlwaysReady`- Some commands, e.g. Test Unit Ready, returns PAR status. • `ALUA` (default) - Initiators are permitted to send I/O to a LUN regardless of which SP actually owns the LUN.
`-lunzEnabled`	Set whether LUNZ will be enabled. Valid values are: • `yes` (default)

Qualifier	Description
	• `no`
`-unitSerialNumber`	Specify the Unit Serial Number. Valid values are: • `Array` (default) • `LUN` For SCSI-3 interfaces, the Unity Serial Number page (Vital Product Data page 0x80) reports the serial number for the array or LUN.

Example 1

The following command creates an FC initiator for host configuration 1014. The FC initiator receives ID 1021:

```
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.
```

Example 2

The following command creates an iSCSI initiator for host configuration Host_3. The iSCSI initiator receives ID 1022:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! -sslPolicy accept /
remote/initiator create -host Host_3 iqn.1000-05.com.fancy:win-123456
-type iscsi
```

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

ID = 1022
Operation completed successfully.
```

Example 3

The following command creates an iSCSI initiator for "Host_3" with:

- A source type of "OpenNative"
- A failover mode of "PassiveAlwaysReady"
- LUNZ disabled
- And an "Array" Unit Serial Number

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/initiator
create -host Host_3 -uid iqn.1993-08.com.microsoft:win -type iscsi -
```

```
sourceType OpenNative -failoverMode PassiveAlwaysReady -lunzEnabled no
-unitSerialNumber Array
```

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

ID = HostInitiator_8
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.

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 the details of 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                   = HostInitiator_7
   Host                 = Host_4
   UID                  = iqn.
1991-05.com.microsoft:cnenfanw4l1c.corp.emc.com
   Initiator type       = iscsi
   Ports logged in      = spb_eth2,spa_eth2
   Ignored              = no
   Health State         = OK (5)
   Health Details       = "The component is operating normally. No
action is required."
   CHAP users           =
   Source type          = Open_Native
   Failover mode        = ALUA
   LUNZ                 = yes
   Unit serial number   = Array
```

Change initiator settings

Modify an already created initiator.

Format

```
/remote/initiator -id <value> set [-ignored {yes | no}] [-host
<value>] [-sourceType {HPAutotrespass | OpenNative | SGI |
HPNoAutotrespass | Dell | FujitsuSiemens | Tru64}] [-
failoverMode {AutoTrespass | PassiveNotReady | DMP |
PassiveAlwaysReady | ALUA}] [-lunzEnabled {yes | no}] [-
unitSerialNumber {Array | LUN}]
```

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. Valid values are: • `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 277 explains how to view the IDs of host configurations on the system.
`-sourceType`	Specify the source type for the initiator. Valid values are: • `HPAutotrespass` — HP with Auto-trespass • `OpenNative` — Open native (such as CLARiiON Open) • `SGI` — Silicon Graphics • `HPNoAutotrespass` — HP without Auto-trespass • `Dell` • `FujitsuSiemens` • `Tru64` — Compaq Tru64
`-failoverMode`	Specify the failover mode for the initiator. Valid values are: • `AutoTrespass` — Any media access to the non owning SP is rejected. • `PassiveNotReady` — A command failure during I/O is sent to the non-owning SP. • `DMP` — Quiet trespass on I/O to non owning SP. • `PassiveAlwaysReady` — Some commands, e.g. Test Unit Ready, returns PAR status. • `ALUA` — Initiators are permitted to send I/O to a LUN regardless of which SP actually owns the LUN.
`-lunzEnabled`	Set whether LUNZ will be enabled. Valid values are: • `yes`

Qualifier	Description
	• `no`
`-unitSerialNumber`	Specify the Unit Serial Number. Valid values are: • `Array` • `LUN` For SCSI-3 interfaces, the Unity Serial Number page (Vital Product Data page 0x80) reports the serial number for the array or LUN.
`-force`	Specify to bypass the validation of setting a new host when there are already storage resources associated with the host and attached to the initiator. If you want to delete a stale initiator for which the associated host has LUN access and as such those LUNs cannot be deleted, you will need to ignore the associated host by setting the stale initiator to an empty host with this `-force` option.

Example

The following command changes the source type, failover mode, LUNZ settings, and Unit Serial Number of the initiator:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/initiator -
id HostInitiator_6 set -sourceType HPAutotrespass -failoverMode
PassiveNotReady -lunzEnabled yes -unitSerialNumber Array
```

```
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 70 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`

Table 70 Initiator path attributes (continued)

Attribute	Description
`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. • `Critical failure (25)` — Failed and recovery may not be possible. This condition has resulted in data loss and should be remedied immediately.

Table 70 Initiator path attributes (continued)

Attribute	Description
	• `Non-recoverable error (30)` — Completely failed and cannot be recovered.
`Health details`	Additional health information. See Health details on page 702, for health information details.

View initiator paths

View a list of initiators. You can filter on the initiator ID.

Note

The show action command on page 23 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
       Registration method = ESX
       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 reverse CHAP for mutual CHAP authentication on page 194 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 71 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. Valid values are: • `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. Valid values are: • `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.

Qualifier	Description
-secretFormat	Specifies the CHAP input format. Valid values are: • ascii(default) — ASCII format • hex — Hexadecimal 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 23 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 iSCSI connections

Identifies iSCSI connections between destination SPs and arrays to the source system that are required to create iSCSI connection paths.

Note

Only one iSCSI connection can be created at a time. Therefore, only one source system can be managed for one migration operation. If a migration operation is already completed, you must create a new iSCSI connection with new paths.

The following table lists the attributes for iSCSI connections.

Table 72 iSCSI connection Attributes

Attribute	Description
ID	ID of the iSCSI connection.
Name	Name of the iSCSI connection.
Description	Description of the iSCSI connection.

Create an iSCSI connection

Create an iSCSI connection.

Note

Only one iSCSI connection can be created at a time. Therefore, only one source system can be managed for one migration operation. If a migration operation is already completed, you must create a new iSCSI connection with new paths.

Format

```
/remote/iscsi/connection create -name <value> [-descr <value>]
[-async]
```

Action qualifiers

Qualifier	Description
-name	Specifies the iSCSI connection name.
-descr	Specifies the iSCSI connection description.
-async	Run the operation in asynchronous mode.

Example

The following command creates an iSCSI connection.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/iscsi/connection create –name myConn –descr "Connection for lun_1 importing"
```

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

ID = iscsi_conn_1
Operation completed successfully.
```

View iSCSI connection settings

View details for existing iSCSI connections.

Format

```
/remote/iscsi/connection [{-id <value> | -name <value>}] show
```

Object qualifiers

Qualifier	Description
-id	Type the ID of the iSCSI connection.
-name	Type the unique name of the iSCSI connection.

Example

This example shows all iSCSI connections.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/iscsi/connection show -detail
```

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

1:    ID                            = iscsi_conn_1
      Name                          = Old Array
      Description                   = LUN 1 import
```

Change iSCSI connection settings

Change the current iSCSI connection settings.

Format

```
/remote/iscsi/connection {–id <value> | -name <value>} set -descr <value> [-async]
```

Object qualifiers

Qualifier	Description
`-id`	Type the ID of the iSCSI connection.
`-name`	Type the unique name of the iSCSI connection.

Action qualifiers

Qualifier	Description
`-descr`	Type the iSCSI connection description.
`-async`	Run the operation in asynchronous mode.

Example

The following command changes the description for the iSCSI connection.

```
uemcli uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/
iscsi/connection -id iscsi_conn_1 set -descr copyconnection
```

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

Operation completed successfully.
```

Delete an iSCSI connection

Deletes an existing iSCSI connection.

Note

When you delete an iSCSI connection, any iSCSI connection paths associated with the iSCSI connection are also deleted.

Format

```
/remote/iscsi/connection {-id <value> | -name <value>} delete
[-async]
```

Object qualifiers

Qualifier	Description
`-id`	Type the ID of the iSCSI connection you want to delete.
`-name`	Type the unique name of the iSCSI connection you want to delete.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.

Example

The following command deletes the "iscsi_conn_1" iSCSI connection.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/iscsi/
connection -id iscsi_conn_1 delete
```

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

Operation completed successfully.
```

Manage iSCSI connection paths

The connection iSCSI path to a remote system includes IP address, TCP port, and a list of iSCSI interfaces on the storage system from which outgoing iSCSI connections are established. An iSCSI connection can have one or more iSCSI paths configured.

Note

If the source system has an iSCSI address which contains CHAP credentials, you must remove the CHAP credentials from the iSCSI address before migration, and then restore the CHAP credentials once migration is complete.

The following table lists the attributes for iSCSI connection paths.

Table 73 iSCSI connection path Attributes

Attribute	Description
`Index`	Number of the iSCSI path within the iSCSI connection.
`iSCSI connection`	ID of the iSCSI connection.
`iSCSI connection name`	Name of the iSCSI connection.
`iSCSI path description`	Description of the iSCSI path.
`Remote iSCSI address`	IP address of the iSCSI destination on the remote system.
`Remote iSCSI port`	TCP port of the iSCSI destination on the remote system.
`Local iSCSI interfaces`	List of identifiers of the iSCSI interfaces on the local storage system.

Create an iSCSI connection path

Creates a new iSCSI path and adds it to a specified iSCSI connection.

Format

```
/remote/iscsi/connection/path create {-connection <value> | -connectionName <value>} [-descr <value>] -addr <value> [-port <value>] -if <value> [-async]
```

Action qualifiers

Qualifier	Description
`-connection`	Type the ID of the iSCSI connection where you want to add a path.

Qualifier	Description
`-connectionName`	Type the unique name of the iSCSI connection where you want to add a path.
`-descr`	Type the iSCSI path description.
`-addr`	Type the IP address of the remote system iSCSI destination. **Note** Do not specify an iSCSI portal address which only redirects the connection to another address. Unity does not support iSCSI redirection.
`-port`	The default TCP port is 3260. If the port number is different from the default, type the TCP port of the remote system iSCSI destination.
`-if`	Specify a comma-separated list of iSCSI interfaces on the local source system. **Note** You can find existing iSCSI interfaces information by using the `/net/if show` command. If a system has two SPs, make sure that you specify iSCSI network interfaces for both SPs.
`-async`	Run the operation in asynchronous mode.

Example

The following command creates an iSCSI path for the "iscsi_conn_1" iSCSI connection.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/iscsi/connection/path create -connection iscsi_conn_1 -addr 10.0.0.4 -if if_1,if_2
```

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

Operation completed successfully.
```

View iSCSI connection path settings

View details for existing iSCSI connection paths.

Format

`/remote/iscsi/connection/path [{-connection <value> | -connectionName <value>}] show`

Object qualifiers

Qualifier	Description
`-connection`	Type the ID of the iSCSI connection.
`-connectionName`	Type the unique name of the iSCSI connection.

Example

This example shows all iSCSI connection paths.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/iscsi/
connection/path -connection iscsi_conn_1 show -detail
```

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

1:     Index                        = 1
       iSCSI connection             = iscsi_conn_1
       iSCSI connection name        = MyConn
       iSCSI path description       = SP 2 node 1
       Remote iSCSI address         = 10.0.0.4
       Remote iSCSI port            = 3260
       Local iSCSI interfaces       = IF_1,IF_2

2:     Index                        = 2
       iSCSI connection             = iscsi_conn_1
       iSCSI connection name        = MyConn
       iSCSI path description       = SP 1 node 2
       Remote iSCSI address         = 10.0.0.6
       Remote iSCSI port            = 3260
       Local iSCSI interfaces       = IF_1,IF_2
```

Delete an iSCSI connection path

Deletes an existing iSCSI connection path.

Note

When you delete an iSCSI connection, any iSCSI connection paths associated with that iSCSI connection are also deleted. You do not need to manually the delete the paths.

Format

```
/remote/iscsi/connection/path {-connection <value> | -connectionName <value>} -index <value> delete [-async]
```

Object qualifiers

Qualifier	Description
-connection	Type the ID of the iSCSI connection that has the path you want to delete.
-connectionName	Type the unique name of the iSCSI connection that has the path you want to delete.
-index	Type the number of the iSCSI path that you want to delete from the iSCSI connection.

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.

Example

The following command deletes the "1" path from the "iscsi_conn_1" iSCSI connection.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/iscsi/connection/path -connection iscsi_conn_1 –index 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 74 Remote system attributes

Attribute	Description
`ID`	ID of the remote system.
`Model`	Model number of the remote system.
`Serial number`	Serial number of the remote system.
`Address`	Network name or management IP address of the remote system.
`Alternate management address`	An alternative 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. • `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.

Table 74 Remote system attributes (continued)

Attribute	Description
	▪ 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. • `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.
`Source user password`	For storage systems that are the source in a replication session, the user password that is used to access the system.
`Local interfaces`	The list of local interface identifiers used to create the interconnection between the two systems.
`Remote interfaces`	The list of remote interface identifiers used to create the interconnection between 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.
`Connection type`	The type of connection with the remote system. Valid values are: • `sync` • `async` • `both`
`Synchronous FC ports`	The fibre channel ports enabled for synchronous replication. **Note** For a local system (RS_0), this field will appear empty only when there are no FC ports. For remote systems, this will be empty when the connection type is asynchronous.

Create remote system configurations

Configures a remote system configuration for the local system to access.

Note

For a source VNX system with two control stations, the home directory of the sysadmin user, which is used in configuring the import connection, must exist on the primary control station of the VNX.

Format

```
/remote/sys create -addr <value> [-type VNX] -srcUsername
<value> {-srcPassword <value> | -srcPasswordSecure} -
dstUsername <value> {-dstPassword <value> | -dstPasswordSecure}
[-connectionType {sync | async | both}]
```

Action qualifiers

Qualifier	Description
`-addr`	Specify the network name or IP address of the remote system.
`-type`	Specify the remote system type. Valid values are: • `VNX`
`-srcUsername`	For systems that are the source in a replication, type the username that is used to access the system.
`-srcPassword`	For systems that are the source in a replication, 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 or VNX in an import session, specify the username that is used to access the system.
`-dstPassword`	For systems that are the destination in a replication session or VNX in an import session, specify 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.
`-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:

- 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_65536:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/sys create -
addr 10.64.75.10 -type VNX -dstUsername admin1 -dstPassword
Password789!
```

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

ID = RS_65536
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 23 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 -
detail
```

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

1:      ID                             = RS_1
        Address                        = 10.2.3.1
        Alternate Management Address =
        Model                          = Unity 300
        Serial number                  = FCNC987654321
        Connection type                = async
        Local interfaces               = N/A
        Remote interfaces              = N/A
        Operational status             = OK (0x2)
        Health state                   = OK (5)
        Health details                 = "Communication with the
replication host is established. No action is required."
        Synchronous FC ports           = spb_fc4, spa_fc4
```

Change settings for remote storage systems

Changes the configuration settings for a remote system.

NOTICE

If a replication connection already exists and you plan to add a different mode of file replication, do not attempt to create a new connection. Change the existing replication connection mode to Both. Also, ensure that you have the appropriate interface types configured to support both asynchronous replication (eth2, eth3) and synchronous replication (sync replication mgmt port).

Format

/remote/sys -id *<value>* set [-addr *<value>*] [-dstUsername *<value>* { -dstPassword *<value>* | -dstPasswordSecure }] [-connectionType {sync | async | both}]

Object qualifier

Qualifier	Description
-id	Type the ID of the remote system configuration to change.

Action qualifiers

Qualifier	Description
-addr	Type the network name or management IP address of the remote system.
-dstUsername	Type the username that is used to access the remote system.
-dstPassword	Type the user password that is used to access the remote system.
-dstPasswordSecure	Specify the password in secure mode - the user will be prompted to input the password.

Qualifier	Description
`-connectionType`	Specify this qualifier to indicate the type of replication connection. Valid values are async, sync, or both.

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 -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.
```

Cabinet level unplanned failover of replication sessions

Execute a failover of all NAS server synchronous replication sessions from the remote system to the local system (unplanned failover). Replication sessions of file systems created on the affected NAS servers will also fail over automatically.

Format

```
/remote/sys -id <value> failover [-force]
```

Object qualifiers

Qualifier	Description
`-id`	Type the ID of the remote system from which to failover its NAS server synchronous replication sessions.

Action qualifiers

Qualifier	Description
`-force`	Specifies whether to skip checking the network connection to the remote system. Required when the network connection is healthy. No values are allowed.

Example

The following command executes a cabinet level unplanned failover replication operation issued for a Unity system:

```
uemcli /remote/sys -id RS_1 failover
```

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

ID = RS_1
Operation completed successfully.
```

Note

After an unplanned failover, the NAS servers and file systems on the original source system must be updated to reflect the new status. If there is a large number of NAS servers and file systems, this change may take several minutes to complete. During this period, resume and failback operations of the synchronous replication sessions will not work. It is recommended to wait for all of the updates to complete before running a resume or failback operation. There is no impact to data access while this update is occurring.

Manage VMware vCenter

Manage VMware vCenter servers.

The following table lists the attributes for VMware vCenter.

Table 75 VMware vCenter attributes

Attribute	Description
`ID`	ID of the VMware virtual center
`Address`	Domain name or IP address of VMware vCenter.

Table 75 VMware vCenter attributes (continued)

Attribute	Description
`User name`	Name of the administrator account on the VMware vCenter.
`Password`	Password of the administrator account on the VMware vCenter.
`Description`	Description of the VMware vCenter.
`VASA provider state`	Indicates whether the system is registered as a VASA provider in vCenter. Values are: • `Registered` • `Not registered` • `Not supported` **Note** Automatic VASA registration is not supported on vSphere versions earlier than 6.0. The storage system can be registered as a VASA provider with only one vCenter at a time.
`Local username`	The username of the local account that vSphere will use to register the system as a VASA provider. **Note** It is recommended that you create a new user with the `/user/account` command and set the role to *vmadmin*.
`Local password`	The password of the local account that vSphere will use to register the system as a VASA provider.

Create VMware vCenter

Adds the vCenter credentials and discovers any ESXi host managed by that vCenter. The vCenter 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>] [-
registerVasaProvider {yes -localUsername <value> {-localPasswd
<value> | -localPasswdSecure} | no}]
```

Action qualifier

Qualifier	Description
`-addr`	Domain name or IP address or domain name of the VMware vCenter.

Qualifier	Description
`-username`	Specify the VMware administrator username used to access the VMware vCenter.
`-passwd`	Specify the VMware administrator password used to access the VMware vCenter.
`-passwdSecure`	Specify the password in secure mode. The user will be prompted to input the password.
`-descr`	Specify the description of the VMware vCenter server.
`-registerVasaProvider`	Specify to register the system as a VASA provider with this vCenter server. Valid values are: • `yes` • `no`
`-localUsername`	Specify the username of the system account that will be used by vCenter to register the system as a VASA provider. **Note** It is recommended that you create a new user with the `/user/account` command and set the role to *vmadmin*. The storage system can be registered as a VASA provider with only one vCenter at a time.
`-localPasswd`	Specify the password of the system account that will be used by vCenter to register the system as a VASA provider.
`-localPasswdSecure`	Specify the VASA password in secure mode, which requires the user to input the password when prompted.

Example 1

The following command adds virtual center credentials:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /virt/vmw/vc create
-addr 10.11.11.111 -username administrator@vsphere.local -passwd xxx -
descr "Add vCenter"
```

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

ID = VC_1
Operation completed successfully
```

Example 2

The following command adds a vCenter and registers the storage system as a VASA provider.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /virt/vmw/vc create
-address 10.11.11.111 -username root -passwd xxx -descr "Add virtual
```

center" -registerVasaProvider yes -localUsername admin -localPasswd Password321

```
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 vCenter server

Modifies the credentials or description of the existing vCenter server. In order to execute this command the user must have an 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 VMware administrator username.
-passwd	Specifies the VMware administrator 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 vCenter server:

uemcli /virt/vmw/vc -id VC_1 set -descr "This vCenter manages 2 ESXi hosts"

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

ID = VC_1
Operation completed successfully.
```

Delete an existing vCenter server

Removes an existing VMware vCenter server and its associated ESXi hosts.

Note

If the Unity system is registered as a VASA provider in vCenter and you delete the vCenter from Unity, the Unity system will be unregistered as a VASA provider from vCenter.

Format

```
/virt/vmw/vc -id <value> delete
```

Object qualifier

Qualifier	Description
`-id`	Identifies the VMware vCenter server.

Example

The following example deletes an existing vCenter server and any of its associated ESXi hosts.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /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 vCenter servers

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 vCenter servers.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /virt/vmw/vc show
```

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

1:      ID                         = VC_1
        Address                    = 10.1.1.1
        Description                = This vCenter manages 2 ESXi hosts
        VASA provider state        = yes
```

Refresh all vCenter servers

Rescan details of all configured VMware vCenter servers.

Format

```
/virt/vmw/vc refresh [-scanHardware]
```

Object qualifier

Qualifier	Description
`-id`	Specify the ID of the vCenter. If not specified, all attached vCenters are refreshed.
`-scanHardware`	Specify to rescan hardware changes (this takes additional time).

Example

The following example rescans all vCenters.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /virt/vmw/vc refresh
-scanHardware
```

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

Operation completed successfully.
```

Manage ESXi hosts

Manage VMware ESXi hosts.

The following table lists the attributes for ESXi hosts.

Table 76 ESXi host attributes

Attribute	Description
`ID`	ID of the ESXi host.
`Name`	Name of the ESXi host.
`Address`	Domain name or IP address of ESXi host.
`Virtual center`	Identifier of the VMware VCenter server managing the ESXi host.
`Username`	Name of the user account on the ESXi host.
`Password`	Password of the user account on the ESXi host.
`Description`	Description of the ESXi host.
`NFSv4 supported`	Indicates if the NFSv4 protocol is supported for the host. Valid values are: • `yes` • `no`
`NFS username`	Displays the NFS user authentication information configured for the ESXi host. The same username should be configured on the

Table 76 ESXi host attributes (continued)

Attribute	Description
	VMware NFS datastore in order to enable secure NFS access with Kerberos for that datastore.

Create an ESXi host

Adds a VMware ESXi host.

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 ESXi host.
-vc	Identifies the VMware vCenter server.
-username	Specifies the username used to access the VMware ESXi host.
-passwd	Specifies the password used to access the VMware ESXi host.
-passwdSecure	Specifies the password in secure mode - the user will be prompted to input the password.
-descr	Specifies the description of the VMware ESXi host.
-resolveConflicts	Specifies the option to resolve IP address or initiator conflicts interactively. Valid values are yes or no (default).

Example 1

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /virt/vmw/esx create
-addr 10.1.1.1 -username root -passwd xxx -descr "My ESXi host"
```

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

ID = ESX_1
Operation completed successfully
```

Example 2

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /virt/vmw/esx create
-addr 10.1.1.1 -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 ESXi host credentials

Changes ESXi host 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 ESXi host.

Action qualifier

Qualifier	Description
`-descr`	Specifies the comment or description.
`-username`	Specifies the username used to access the VMware ESXi host.
`-passwd`	Specifies the password used to access the VMware ESXi host.
`-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 ESXi host in order for Unisphere to contact the ESXi host directly. **Note** This is only applicable for standalone ESXi hosts.

Example

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /virt/vmw/esx -id
ESX_1 set -descr "Changing ESXi host description"
```

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

ID = ESX_1
Operation completed successfully.
```

Delete ESXi host credentials

Deletes ESXi host credentials. This will also remove access from the specified host to any VMware datastores or protocol endpoints that are associated with it.

Format

```
/virt/vmw/esx -id <value> delete
```

Object qualifier

Qualifier	Description
`-id`	Identifies the ESXi host.

Example

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /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 ESXi hosts

Displays a list of all configured VMware ESXi hosts.

Format

```
/virt/vmw/esx [{-id <value> | -vc <value>}] show
```

Object qualifier

Qualifier	Description
`-id`	Identifies the VMware ESXi host.
`-vc`	Identifies the VMware vCenter server.

Example

The following example shows how to display all of the ESXi hosts on the vCenter connected to the system.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /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.aa.bb.com
        vCenter          = VC_1
        Address          = 10.10.10.100
        Description      =
        NFSv4 supported  = yes
        NFS username     = root


2:      ID               = ESX_2
        Name             = nlpc12241.xx.yy.com
        vCenter          = VC_1
        Address          = 10.10.10.101
        NFSv4 supported  = no
        NFS username     =
```

Discover all ESXi hosts

Lists all VMware ESXi hosts 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 ESXi hosts automatically.

Example

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /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 ESXi host

Rescans details of a VMware ESXi host.

Format

```
/virt/vmw/esx [-id <value>] refresh [-scanHardware]
```

Object qualifier

Qualifier	Description
`-id`	Identifies the ESXi host. If an ID is not specified, all virtualization objects are rescanned.

Action qualifier

Qualifier	Description
`-scanHardware`	Specify to rescan hardware changes also (takes additional time).

Example

The following command rescans the hardware to discover additional ESXi hosts.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /virt/vmw/esx
refresh -scanHardware
```

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


Operation completed successfully.
```

Virtual machine

Manage VMware virtual machines.

The following table lists the attributes for Virtual machine.

Table 77 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`	ESXi hosts containing the virtual machine.
`OS`	Guest operating system.
`State`	Virtual machine power state. Valid values are:

Table 77 Virtual machine attributes (continued)

Attribute	Description
	• Powered on • Powered off • Suspended

View all existing virtual machines

Displays a list of all existing virtual machines on existing ESXi hosts on the Unity system.

Format

```
/virt/vmw/vm [{-id <value> | -esx <value>}] show
```

Object qualifier

Qualifier	Description
-id	Identifies the virtual machine.
-esx	Identifies the ESXi host.

Example

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /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 stored on the Unity system.

The following table lists the attributes for VM hard disks.

Table 78 VM hard disk attributes

Attribute	Description
Name	Name of the hard disk.
Type	Type of the VM hard disk.

Table 78 VM hard disk attributes (continued)

Attribute	Description
`Capacity`	VM hard disk capacity.
`Datastore`	Associated datastore.

View all hard disks

Displays hard disk properties for a specified virtual machine stored on the Unity system.

Format

```
/virt/vmw/vmdevice -vm <value> show
```

Object qualifier

Qualifier	Description
`-vmId`	Identifies the virtual machine.

Example

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /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 contains the following topics:

Manage Storage Processor (SP)

The following table lists the health state values for the storage processor (SP) in Normal mode.

Table 79 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 80 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.

Table 80 Storage processor health state values (Service/Rescue mode) (continued)

Code	Health state	Reason(s)
		• The SSD in the SP has faulted. • The entire blade in the SP has faulted. • The fibre cable connection in the SP has faulted. • 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 drive in the storage processor has faulted. • One of the first four drives have mismatched types. • One of the first four drives has an invalid block size. • One of the first four drives has a 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
```

```
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
      UUID           = 421DB2B2-6AAC-BB48-73DE-513390292444
      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 drive.

Table 81 Physical drive health state values

Code	Health state	Reason(s)
0	Unknown	• The health of the component cannot be determined.
5	OK	• The drive is operating normally. • The drive slot is empty.
10	Degraded/Warning	• The drive is resynchronizing with the system. • The drive cannot be used because the system has exceeded the maximum number of allowable drives.
15	Minor failure	• The drive is inserted in the wrong slot. • The drive is removed. • The drive is offline.

Table 81 Physical drive health state values (continued)

Code	Health state	Reason(s)
20	Major failure	• The drive has faulted. • The drive is unsupported.

Table 82 Virtual disk health state values

Code	Health state	Reason(s)
0	Unknown	• The health of the component cannot be determined.
5	OK	• The virtual disk is operating normally.
7	OK_BUT	• The virtual disk was originally configured for a different storage system. • The virtual disk was originally configured for a different storage pool.
20	Major failure	• The virtual disk is not accessible. • The virtual disk is too small. • The virtual disk is too large. • The virtual disk failed due to system or I/O error.

View disk

View existing drives.

Format

```
/env/disk [{-id <value> | -pool <value> | -fastcache | -
unused}] show
```

Object qualifier

Qualifier	Description
-id	ID of the drive.
-pool	Shows the drive that belong to the specified pool.
-fastcache	Shows the drives used in FAST Cache.
-unused	Shows unused drives.

Example 1

The following command displays the basic attributes of all drives on a physical deployment.

```
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
```

Example 2

The following command displays the details of all drives on a physical deployment.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/disk show -detail

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

1:    ID                    = dae_1_2_disk_59
      Enclosure             = dae_1_2
      Slot                  = 59
      Bank slot             = C19
      Name                  = Disk 59
      Health state          = OK (5)
      Health details        = "The component is operating normally.
No action is required."
      Type                  = SAS
      Tier                  = performance
      Capacity              = 881132310528 (820.6G)
      Rotational speed      = 10000 rpm
      User capacity         = 797989670912 (743.1G)
      Used by FAST Cache    = no
      Pool ID               = Unconfigured
      Pool                  = Unconfigured
      Current speed         = 6 Gbps
      Maximum speed         = 6 Gbps
      Manufacturer          = SEAGATE
      Model                 = ST990080 CLAR900
      Vendor capacity       = 966367641600 (900.0G)
      Part number           = 005049206PWR
      Serial number         = 6XS3A9CG
      Firmware revision     = CS19
      WWN                   =
06:00:00:00:05:00:00:00:01:00:00:00:00:00:00:03
      Days remaining to EOL = 1497
```

Example 3

The following command displays the details of all drives on a single-SP virtual deployment.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/disk show -detail

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

1:     ID                   = vdisk_1
       SCSI ID              = 0:3
       Name                 = Virtual Disk 1
       Health state         = OK (5)
       Health details       = "The component is operating normally.
No action is required."
       Type                 = virtual
       Tier                 = capacity
       Capacity             = 268435456000 (250.0G)
       Rotational speed     =
       User capacity        = 268435435520 (249.9G)
       Pool ID              = pool_1
       Pool                 = StoragePool00
       Current speed        =
       Maximum speed        =
       Manufacturer         = VMware
       Model                = Virtual disk
       Vendor capacity      = 268435456000 (250.0G)
       WWN                  =
06:00:00:00:05:00:00:00:04:00:00:00:00:00:00:03
```

Example 4

The following command displays the details of all drives on a dual-SP virtual deployment.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/disk show -detail

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

1:     ID                   = vdisk_1
       SCSI ID SPA          = 0:3
       SCSI ID SPB          = 0:4
       Name                 = Virtual Disk 1
       Health state         = OK (5)
       Health details       = "The component is operating normally.
No action is required."
       Type                 = virtual
       Tier                 = capacity
       Capacity             = 268435456000 (250.0G)
       Rotational speed     =
       User capacity        = 268435435520 (249.9G)
       Pool ID              = pool_1
       Pool                 = StoragePool00
       Current speed        =
       Maximum speed        =
       Manufacturer         = VMware
       Model                = Virtual disk
       Vendor capacity      = 268435456000 (250.0G)
       WWN                  =
06:00:00:00:05:00:00:00:04:00:00:00:00:00:00:03
```

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.
```

Change disk settings (virtual deployments only)

Change settings of an existing disk.

Format

```
/env/disk -id <value> set [-async] [-name <value>] [-tier
<value>]
```

Object qualifier

Qualifier	Description
`-id`	Disk identifier.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-name`	Specify the new name for the disk.
`-tier`	Specify the new tier. Valid values are: • capacity • performance • extreme **Note** Disks without a tier cannot be used for pool provisioning.

Example

The following command changes the name of the virtual disk with the ID "vdisk_1".

`uemcli -d 10.0.0.2 -u Local/joe -p MyPassword456! /env/disk -id vdisk_1 set -name "High-performance storage"`

```
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 83 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 84 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 85 Link control card health state values

Code	Health state	Reason(s)
0	Unknown	- The health of the component cannot be determined.
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 86 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. - 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 87 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. • 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_1
      Slot                         = 0
      Name                         = DAE 0 1
      Health state                 = OK (5)
      Health details               = "The component is operating
normally. No action is required."
      Manufacturer                 = USI
      Model                        = 25 DRIVE 6G SAS DERRINGER DAE
      Part number                  = 100-562-712
      Serial number                = US1D1102500097
      Power (Present)              = 232 watts
      Power (Rolling Average)      = 231 watts
      Temperature  (Present)       = 84° F (29° C)
      Temperature (Rolling Average) = 84° F (29° C)
      Bus                          = 0
      Enclosure number             = 1
```

Manage disk processor enclosure (DPE)

The following table lists the health state values for system disk processor enclosures (DPEs).

Table 88 Disk processor enclosure health state values

Code	Health state	Reason(s)
0	Unknown	• The health of the component cannot be determined.
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.

Table 88 Disk processor enclosure health state values (continued)

Code	Health state	Reason(s)
		• 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 details of the system DPE.

Format

```
/env/dpe [-id <value>] show
```

Object qualifier

Qualifier	Description
`-id`	ID of the DPE.

Example 1 (physical deployments only)

The following command displays the system DPE information:

```
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
      Slot                            = 0
      Name                            = DPE
      Health state                    = OK (5)
      Health details                  = "The component is operating 
normally. No action is required."
      Manufacturer                    = 
      Model                           = BC DPE NO I/O DUAL SP 25 DRV 
6C
      Part number                     = 100-542-441-03
      Serial number                   = FCNBV131000114
      Power (Present)                 = 361 watts
      Power (Rolling Average)         = 362 watts
      Temperature  (Present)          = 84° F (29° C)
      Temperature (Rolling Average) = 84° F (29° C)
```

Example 2 (virtual deployments only)

The following command displays the system DPE information:

```
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
      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 89 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 System Status Card (physical deployments only)

The following table lists the health state values for System Status Cards (SSC).

Table 90 SSC health state values

Code	Health state	Reason(s)
0	`Unknown`	• The health of the component cannot be determined.
5	`OK`	• The SSC is operating normally.
20	`Major failure`	• The SSC has faulted. • The SSD is missing.

View SSC

View a list of System Status Cards (SSC).

Format

`/env/ssc [-id <value>] show`

Object qualifier

Qualifier	Description
`-id`	ID of the SSC.

Example

The following command displays the details of the system status card.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/ssc show -
detail
```

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

1:     ID             = dae_0_3_ssc
       Enclosure      = dae_0_3
       Slot           = 0
       Name           = DAE 0 3 System Status Card
       Health state   = OK (5)
       Health details = "The component is operating normally. No
action is required."
       Manufacturer   = EMC
       Model          = NAGA 120 DRIVE 12G SAS SSC FRU
       Part number    = 303-340-000C-00
       Serial number  = CF2BW162200072
```

Manage fan modules (physical deployments only)

The following table lists the health state values for the system fan modules.

Table 91 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 92 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 340 explains how to commit an I/O module.

Table 92 I/O module attributes (continued)

Attribute	Description
	• `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 more 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`	Part Number on the I/O module.
`Serial number`	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

The show action command on page 23 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 contains the following topics:

Configure custom pools

Pools are the groups of drives on which you create storage resources. Configure 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 drive used to provide the storage.
- (dual-SP virtual deployments only) RAID level implemented for the storage.

Note

Before you create storage resources, you must configure at least one pool.

The following table lists the attributes for pools:

Table 93 Custom pool attributes

Attribute	Description
`ID`	ID of the pool.
`Name`	Name of the pool.
`Type`	Pool type. Valid values are: • Dynamic • Traditional
`Description`	Brief description of the pool.
`Total space`	Total storage capacity of the pool.
`Current allocation`	Amount of storage in the pool allocated to storage resources.
`Preallocated space`	Amount of storage space reserved in the pool by storage resources for future needs to make writes more efficient. The pool may be able to reclaim some of this space if total pool space is running low. This value equals the sum of the `sizePreallocated` values of each storage resource in the pool.
`Remaining space`	Amount of storage in the pool not allocated to storage resources.
`Subscription`	For thin provisioning, the total storage space subscribed to the pool. All 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, pools can be over provisioned to support more storage capacity than they actually possess.

Table 93 Custom pool attributes (continued)

Attribute	Description
	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 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 drives on the system, including the number of drives of each type, in the pool. If FAST VP is installed, you can mix different types of drives to make a tiered pool. However, SAS Flash 4 drives must be used in a homogeneous pool.
Number of drives	Total number of drives in the pool.
Number of unused drives	Number of drives in the pool that are not being used.
RAID level (physical deployments only)	RAID level of the drives in the pool.
Stripe length (physical deployments only)	Number of drives the data is striped across.
Rebalancing	Indicates whether a pool rebalancing is in progress. Valid values are: • 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 • no
Health state	Health state of the pool. The health state code appears in parentheses. Valid values are: • 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.

Table 93 Custom pool attributes (continued)

Attribute	Description
	- 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 drives 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 (physical deployments only)	Indicates whether FAST Cache is enabled on the pool. Valid values are: - yes - no
Non-base size used	Quantity of storage used for thin clone and snapshot data.
Auto-delete state	Indicates the state of an auto-delete operation on the pool. Valid values are: - 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 pool, the auto-delete operation sets the auto-delete state for that watermark to Could not reach HWM , and generates an alert. - Failed
Auto-delete paused	Indicates whether an auto-delete operation is paused. Valid values are: - yes - no
Auto-delete pool full threshold enabled	Indicates whether the system will check the pool full high water mark for auto-delete. Valid values are: - yes

Table 93 Custom pool attributes (continued)

Attribute	Description
	- `no`
`Auto-delete pool full high water mark`	The pool full high watermark on the pool.
`Auto-delete pool full low water mark`	The pool full low watermark on the pool.
`Auto-delete snapshot space used threshold enabled`	Indicates whether the system will check the snapshot space used high water mark for auto-delete. Valid values are: - `yes` - `no`
`Auto-delete snapshot space used high water mark`	High watermark for snapshot space used on the pool.
`Auto-delete snapshot space used low water mark`	Low watermark for snapshot space used on the pool.
`Data Reduction space saved` (physical deployments only)	Storage size saved on the pool by using data reduction. **Note** Data reduction is available for thin LUNs and thin file systems in an All-Flash pool only. The thin file systems must be created on Unity systems running version 4.2.x or later.
`Data Reduction percent` (physical deployments only)	Storage percentage saved on the pool by using data reduction. **Note** Data reduction is available for thin LUNs and thin file systems in an All-Flash pool only. The thin file systems must be created on Unity systems running version 4.2.x or later.
`Data Reduction ratio` (physical deployments only)	Ratio between data without data reduction and data after data reduction savings. **Note** Data reduction is available for thin LUNs and thin file systems in an All-Flash pool only. The thin file systems must be created on Unity systems running version 4.2.x or later.
`All flash pool`	Indicates whether the pool contains only Flash drives. Valid values are:

Table 93 Custom pool attributes (continued)

Attribute	Description
	- yes - no

Create pools

Create a dynamic or traditional pool:

- Both traditional pools and dynamic pools are supported in the CLI and REST API for Unity All-Flash models running OE version 4.2.x or later. The default pool type is dynamic.
- Traditional pools are supported in all Unity hybrid and virtual models. They are also supported in Unity All-Flash models running OE version 4.1.x or earlier.

Format

```
/stor/config/pool create [-async] -name <value> [-type {dynamic
| traditional}] [-descr <value>] {-diskGroup <value> -
drivesNumber <value> [-storProfile <value>] | -disk <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. **Note** Simultaneous commands, asynchronous or synchronous, may fail if they conflict in trying to manage the same system elements.
-name	Type a name for the pool.
-type	(Available only for systems that support dynamic pools) Specify the type of pool to create. Value is one of the following: - dynamic - traditional Default value is dynamic.
-descr	Type a brief description of the pool.
-storProfile (physical deployments only)	Type the ID of the storage profiles, separated by commas, to apply to the pool, based on the type of storage resource that will use the pool and the

Qualifier	Description
	intended usage of the pool. View storage profiles (physical deployments only) on page 377 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 drive 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 a comma-separated list of IDs of the drive groups to use in the pool. Specifying drive groups with different drive types causes the creation of a multi-tier pool. View drive groups on page 381 explains how to view the IDs of the drive groups on the system.
`-drivesNumber` (physical deployments only)	Specify the drive numbers, separated by commas, from the selected drive groups to use in the 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 drive group.
`-disk` (virtual deployments only)	Specify the list of drive IDs, separated by commas, to use in the pool. Specified drives must be reliable storage objects that do not require additional protection.
`-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` (physical deployments only)	Specify whether to enable FAST Cache on the 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:

Qualifier	Description
	• yes • no Default value is yes.
-snapPoolFullHWM	Specify the pool full high watermark for the pool. Valid values are 1-99. Default value is 95.
-snapPoolFullLWM	Specify the pool full low watermark for the 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 pool. Valid values are 1-99. Default value is 95.
-snapSpaceUsedLWM	Specify the snapshot space used low watermark to trigger auto-delete on the pool. Valid values are 0-98. Default value is 20.

Note

Use the Change disk settings (virtual deployments only) on page 328 command to change the assigned tiers for specific drives.

Example 1 (physical deployments only)

The following command creates a dynamic pool. This example uses storage profiles profile_1 and profile_2, six drives from drive group dg_2, and ten drives from drive group dg_28. The configured pool receives ID pool_2.

Note

Before using the stor/config/pool create command, use the /stor/config/profile show command to display the dynamic pool profiles and the /stor/config/dg show command to display the drive groups.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! uemcli /stor/config/
pool create -name MyPool -descr "dynamic pool" -diskGroup dg_2,dg_28 -
drivesNumber 6,10 -storProfile profile_1,profile_2
```

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

```
HTTPS connection

ID = pool_2
Operation completed successfully.
```

Example 2 (physical deployments only)

The following command creates a traditional pool in models that support dynamic pools. This example uses storage profiles tprofile_1 and tprofile_2, five drives from drive group dg_3, and nine drives from drive group dg_28. The configured pool receives ID pool_6.

Note

Before using the `stor/config/pool create` command, use the `/stor/config/profile -traditional show` command to display the traditional pool profiles (which start with "t") and the `/stor/config/dg` show command to display the drive groups.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool
create -name MyPool -descr "traditional pool" -diskGroup dg_3,dg_28 -
drivesNumber 5,9 -storProfile tprofile_1,tprofile_2 -type traditional
```

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

ID = pool_6
Operation completed successfully.
```

Example 3 (physical deployments only)

The following command creates a traditional pool in models that do not support dynamic pools. This example uses storage profiles profile_19 and profile_20, five drives from drive group dg_15, and nine drives from drive group dg_16. The configured pool receives ID pool_5.

Note

Before using the `stor/config/pool create` command, use the `/stor/config/profile show` command to display the traditional pool profiles and the `/stor/config/dg show` command to display the drive groups.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool
create -name MyPool -descr "my big pool" -storProfile
profile_19,profile_20 -diskGroup dg_15,dg_16 -drivesNumber 5,9 -
FASTCacheEnabled yes
```

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

ID = pool_5
Operation completed successfully.
```

Example 4 (virtual deployments only)

The following command creates a traditional pool with two virtual disks, vdisk_0 and vdisk_2 in the Extreme Performance tier. The configured 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
```

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

ID = pool_4
Operation completed successfully.
```

Change pool settings

Change the subscription alert threshold, FAST Cache, and snapshot threshold settings for a pool.

Format

```
/stor/config/pool {-id <value> | -name <value>} set [-async] –
name <value> [-descr <value>] [-alertThreshold <value>] [-
snapPoolFullThresholdEnabled {yes|no}] [-snapPoolFullHWM
<value>] [-snapPoolFullLWM <value>] [-
snapSpaceUsedThresholdEnabled {yes|no}] [-snapSpaceUsedHWM
<value>] [-snapSpaceUsedLWM <value>] [-snapAutoDeletePaused no]
```

Object qualifiers

Qualifier	Description
-id	Type the ID of the pool to change.
-name	Type the name of the pool to change.

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode. Note Simultaneous commands, asynchronous or synchronous, may fail if they conflict in trying to manage the same system elements.
-name	Type a name for the pool.
-descr	Type a brief description of the 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

Qualifier	Description
	subscription space, the system sends an alert. Value range is 50% to 84%.
-FASTCacheEnabled (physical deployments only)	Specify whether to enable FAST Cache on the pool. Value is one of the following: • yes • no
-snapPoolFullThresholdEnabled	Indicate whether the system should check the pool full high water mark for auto-delete. Value is one of the following: • yes • no
-snapPoolFullHWM	Specify the pool full high watermark for the pool. Valid values are 1-99. Default value is 95.
-snapPoolFullLWM	Specify the pool full low watermark for the 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
-snapSpaceUsedHWM	Specify the snapshot space used high watermark to trigger auto-delete on the pool. Valid values are 1-99. Default value is 95.
-snapSpaceUsedLWM	Specify the snapshot space used low watermark to trigger auto-delete on the pool. Valid values are 0-98. Default value is 20.
-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 pool pool_1 to 70%:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool -
id pool_1 -set -alertThreshold 70 -FASTCacheEnabled no
```

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

```
HTTPS connection

ID = pool_1
Operation completed successfully.
```

Add drives to pools

Add new drives to a pool to increase its storage capacity.

Format

```
/stor/config/pool {-id <value> | -name <value>} extend [-async]
{-diskGroup <value> -drivesNumber <value> [-storProfile
<value>] |-disk <value>}
```

Object qualifiers

Qualifier	Description
`-id`	Type the ID of the pool to extend.
`-name`	Type the name of the pool to extend.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-diskGroup` (physical deployments only)	Type the IDs of the drive groups, separated by commas, to add to the pool.
`-drivesNumber` (physical deployments only)	Type the number of drives from the specified drive groups, separated by commas, to add to the 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 drive group.
`-storProfile` (physical deployments only)	Type the IDs of the storage profiles, separated by commas, to apply to the pool. If this option is not specified, a default RAID configuration is selected for each particular drive type in the selected drive 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).
`-disk` (virtual deployments only)	Specify the list of drives, separated by commas, to add to the pool. Specified drives must be reliable storage objects that do not require additional protection.

Example 1 (physical deployments only)

The following command extends pool pool_1 with seven drives from drive group DG_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool –
id pool_1 extend –diskGroup dg_1 –drivesNumber 7 –storProfile
profile_12
```

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

```
HTTPS connection

ID = pool_1
Operation completed successfully.
```

Example 2 (virtual deployments only)

The following command extends 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.
```

View pools

View a list of pools. You can filter on the pool ID.

Note

The show action command on page 23 explains how to change the output format.

Format

`/stor/config/pool {-id <value> | -name <value>}] show`

Object qualifiers

Qualifier	Description
`-id`	Type the ID of a pool.
`-name`	Type the name of a pool.

Example 1 (physical deployments only)

The following command shows details about all pools on a hybrid 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                                             = pool_1
       Name                                            = Performance
       Description                                     = Multi-tier pool
       Total space                                     = 8663754342400 (7.8T)
       Current allocation                              = 0
       Preallocated space                              = 38310387712 (35.6G)
       Remaining space                                 = 8663754342400 (7.8T)
       Subscription                                    = 0
       Subscription percent                            = 0%
       Alert threshold                                 = 70%
       Drives                                            = 5 x 600.0G SAS; 5 x 1.6T SAS
Flash 3
       Number of drives                                  = 10
       RAID level                                        = 5
       Stripe length                                     = 5
       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                              = 0
       Non-base size used                                = 0
       Auto-delete state                                 = Idle
       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 = no
       Auto-delete snapshot space used high water mark   = 25%
       Auto-delete snapshot space used low water mark    = 20%
       Compression space saved                           = 0
       Compression Percent                               = 0%
       Compression Ratio                                 = 1:1
       Data Reduction space saved                        = 0
       Data Reduction percent                            = 0%
       Data Reduction ratio                              = 1:1
       All flash pool                                    = no

2:     ID                                                = pool_2
       Name                                              = Capacity
       Description                                       =
       Total space                                       = 4947802324992 (4.5T)
       Current allocation                                = 3298534883328 (3T)
       Preallocated space                                = 22194823168 (20.6G)
       Remaining space                                   = 4947802324992 (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)
       Non-base 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%
       Compression space saved                           = 4947802324992 (1.5T)
       Compression percent                               = 23%
       Compression ratio                                 = 1.3:1
       Data Reduction space saved                        = 4947802324992 (1.5T)
       Data Reduction percent                            = 23%
       Data Reduction ratio                              = 1.3:1
       All flash pool                                    = no
```

```
 3:    ID                                                 = pool_3
       Name                                               = Extreme Performance
       Description                                        =
       Total space                                        = 14177955479552 (12.8T)
       Current allocation                                 = 0
       Preallocated space                                 = 14177955479552 (12.8T)
       Remaining space                                    = 14177955479552 (12.8T)
       Subscription                                       = 0
       Subscription percent                               = 0%
       Alert threshold                                    = 70%
       Drives                                             = 9 x 1.6T SAS Flash 3; 5 x
400.0G SAS Flash 2
       Number of drives                                   = 14
       RAID level                                         = 5
       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                               = 0
       Non-base size used                                 = 0
       Auto-delete state                                  = Idle
       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  = no
       Auto-delete snapshot space used high water mark    = 25%
       Auto-delete snapshot space used low water mark     = 20%
       Compression space saved                            = 0
       Compression Percent                                = 0%
       Compression Ratio                                  = 1:1
       Data Reduction space saved                         = 0
       Data Reduction percent                             = 0%
       Data Reduction ratio                               = 1:1
       All flash pool                                     = yes
```

Example 2

The following example shows all pools for a model that supports dynamic pools.

uemcli -d 10.0.0.2 -u Local/joe -p MyPassword456! /stor/config/pool show -detail

```
[Response]
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection
1:    ID                                                 = pool_3
      Type                                               = Traditional
      Name                                               = MyPool
      Description                                        = traditional pool
      Total space                                        = 14177955479552 (12.8T)
      Current allocation                                 = 0
      Preallocated space                                 = 38310387712 (35.6G)
      Remaining space                                    = 14177955479552 (12.8T)
      Subscription                                       = 0
      Subscription percent                               = 0%
      Alert threshold                                    = 70%
      Drives                                             = 9 x 1.6T SAS Flash 3; 5 x 400.0G
SAS Flash 2
      Number of drives                                   = 14
      RAID level                                         = 5
      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                              = 0
      Non-base size used                                = 0
      Auto-delete state                                 = Idle
      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 = no
      Auto-delete snapshot space used high water mark   = 25%
      Auto-delete snapshot space used low water mark    = 20%
      Compression space saved                           = 0
      Compression Percent                               = 0%
      Compression Ratio                                 = 1:1
      Data Reduction space saved                        = 0
      Data Reduction percent                            = 0%
      Data Reduction ratio                              = 1:1
      All flash pool                                    = yes

2:    ID                                                = pool_4
      Type                                              = Dynamic
      Name                                              = dynamicPool
      Description                                       =
      Total space                                       = 1544309178368 (1.4T)
      Current allocation                                = 0
      Preallocated space                                = 38310387712 (35.6G)
      Remaining space                                   = 1544309178368 (1.4T)
      Subscription                                      = 0
      Subscription percent                              = 0%
      Alert threshold                                   = 70%
      Drives                                            = 6 x 400.0G SAS Flash 2
      Number of drives                                  = 6
      RAID level                                        = 5
      Stripe length                                     = 5
      Rebalancing                                       = no
      Rebalancing progress                              =
      Health state                                      = OK (5)
      Health details                                    = "The component is operating
normally. No action is required."
      Protection size used                              = 0
      Non-base size used                                = 0
      Auto-delete state                                 = Idle
      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 = no
      Auto-delete snapshot space used high water mark   = 25%
      Auto-delete snapshot space used low water mark    = 20%
      Compression space saved                           = 0
      Compression Percent                               = 0%
      Compression Ratio                                 = 1:1
      Data Reduction space saved                        = 0
      Data Reduction percent                            = 0%
      Data Reduction ratio                              = 1:1
      All flash pool                                    = yes
```

Example 3 (virtual deployments only)

The following command shows details for all 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)
        Preallocated space                                = 38310387712 (35.6G)
        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."
        Non-base 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%
```

Delete pools

Delete a pool.

Format

`/stor/config/pool {-id <value> | -name <value>} delete [-async]`

Object qualifiers

Qualifier	Description
-id	Type the ID of the pool to delete.
-name	Type the name of the pool to delete.

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode. **Note** Simultaneous commands, asynchronous or synchronous, may fail if they conflict in trying to manage the same system elements.

Example

The following deletes pool pool_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool –
id pool_1 delete
```

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

Operation completed successfully.
```

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 pool based on data access patterns.

The following table lists the attributes for FAST VP pool settings.

Table 94 FAST VP pool attributes

Attribute	Description
`Pool`	Identifies the pool.
`Status`	Identifies the status of data relocation on the 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]`

Table 94 FAST VP pool attributes (continued)

Attribute	Description
	where: • value - Identifies the size of the data relocated. • 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 pool scheduled to be moved to a higher storage tier.
Data to move down	The amount of data in the pool scheduled to be moved to a lower storage tier.
Data to move within	The amount of data in the 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.

Table 94 FAST VP pool attributes (continued)

Attribute	Description
	• `value` - Identifies the amount of data in that tier to be rebalanced.
`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> | -poolName <value>}
set [-async] -schedEnabled {yes | no}
```

Object qualifiers

Qualifier	Description
`-pool`	Type the ID of the pool.
`-poolName`	Type the name of the pool.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode. **Note** Simultaneous commands, asynchronous or synchronous, may fail if they conflict in trying to manage the same system elements.
`-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 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 pool.

Format

/stor/config/pool/fastvp [{-pool *<value>* | -poolName *<value>*}] show

Object qualifiers

Qualifier	Description
-pool	Type the ID of the pool.
-poolName	Type the name of the 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 pool.

Format

/stor/config/pool/fastvp {-pool *<value>* | -poolName *<value>*} start [-async] [-rate {low | medium | high}] [-endTime *<value>*]

Object qualifiers

Qualifier	Description
-pool	Type the ID of the pool to resume data relocation.
-poolName	Type the name of the pool to resume data relocation.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode. **Note** Simultaneous commands, asynchronous or synchronous, may fail if they conflict in trying to manage the same system elements.
`-pool`	Type the ID of the 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.
`-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 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 pool.

Format

```
/stor/config/pool/fastvp {-pool <value> | -poolName <value>}
stop [-async]
```

Object qualifiers

Qualifier	Description
`-pool`	Type the ID of the pool.

Qualifier	Description
-poolName	Type the name of the pool.

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.

Example

The following command stops data relocation on 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.
```

Manage pool tiers

Storage tiers allow users to move data between different types of drives in a pool to maximize storage efficiency. Storage tiers are defined by the following characteristics:

- Drive performance.
- Drive capacity.

The following table lists the attributes for storage profiles:

Table 95 Storage tier attributes

Attribute	Description
Name	Storage tier name.
Drives	The list of drive types, and the number of drives 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 drives 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 pool ID.

Note

The show action command on page 23 explains how to change the output format.

Format

```
/stor/config/pool/tier {-pool <value> | -poolName <value>} show
```

Object qualifiers

Qualifier	Description
-pool	Type the ID of a pool.
-poolName	Type the name of a pool.

Example 1 (physical deployments only)

The following command shows tier details about the specified pool:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool/
tier -pool pool_1 show -detail
```

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

1:     Name                  = Extreme Performance
       Drives                = 2 x 200.0G SAS Flash 2; 2 x 800.0G SAS
Flash 2
       Drive type            = SAS Flash
       RAID level            = 10
       Stripe length         = 2
       Total space           = 868120264704 (808.5G)
       Current allocation    = 56371445760 (52.5G)
       Remaining space       = 811748818944 (756.0G)

2:     Name                  = Performance
       Drives                = 15 x 600.0G SAS
       Drive type            = SAS
       RAID level            = 5
       Stripe length         = 5
       Total space           = 7087501344768 (6.4T)
       Current allocation    = 0
       Remaining space       = 7087501344768 (6.4T)

3:     Name                  = Capacity
       Drives                = 8 x 6.0T NL-SAS
       Drive type            = NL-SAS
       RAID level            = 6
       Stripe length         = 8
       Total space           = 35447707271168 (32.2T)
       Current allocation    = 1610612736 (1.5G)
       Remaining space       = 35446096658432 (32.2T)
```

Example 2 (virtual deployments only)

The following command shows details about 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
```

View pool resources

This command displays a list of storage resources allocated in a pool. This can be storage resources provisioned on the specified pool and NAS servers that have file systems allocated in the pool.

The following table lists the attributes for pool resources.

Table 96 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` • `NAS server`
`Pool`	Name of the pool.
`Total pool space used`	Total space in the pool used by a storage resource. This includes primary data used size, snapshot used size, and metadata size. Space in the pool can be freed if snapshots and thin clones for storage resources are deleted, or have expired.
`Total pool space preallocated`	Total space reserved from the pool by the storage resource for future needs to make writes more efficient. The pool may be able to reclaim some of this if space is running low.

Table 96 Pool resources (continued)

Attribute	Description
	Additional pool space can be freed if snapshots or thin clones are deleted or expire, and also if Data Reduction is applied.
`Total pool non-base space used`	Total pool space used by snapshots and thin clones.
`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.

Format

```
/stor/config/pool/sr [{-pool <value> | -poolName <value>}] show
```

Object qualifiers

Qualifier	Description
`-pool`	Type the ID of the pool.
`-poolName`	Type the name of the pool.

Example

The following command shows details for all storage resources associated with the 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                            = File_System_1
         Resource type                   = File System
         Pool                            = pool_1
         Total pool space used           = 53024473088 (49.3G)
         Total pool preallocated         = 15695003648 (14.6G)
         Total pool snapshot space used = 7179124736 (6.6G)
         Total pool non-base space used = 7179124736 (6.6G)
         Health state                    = OK (5)
         Health details                  = "The component is
operating normally. No action is required."

2:       ID                              = sv_1
         Name                            = AF LUN 1
         Resource type                   = LUN
         Pool                            = pool_1
         Total pool space used           = 14448566272 (13.4G)
         Total pool preallocated         = 4610351104 (4.2G)
         Total pool snapshot space used = 4593991680 (4.2G)
         Total pool non-base space used = 4593991680 (4.2G)
         Health state                    = OK (5)
         Health details                  = "The LUN is operating
normally. No action is required."
```

```
3:       ID                             = res_2
         Name                           = File_System_2
         Resource type                  = File System
         Pool                           = pool_1
         Total pool space used          = 117361025024 (109.3G)
         Total pool preallocated        = 3166494720 (2.9G)
         Total pool snapshot space used = 41022308352 (38.2G)
         Total pool non-base space used = 41022308352 (38.2G)
         Health state                   = OK (5)
         Health details                 = "The component is
operating normally. No action is required."

4:      ID                              = sv_2
        Name                            = AF LUN 2
        Resource type                   = LUN
        Pool                            = pool_1
        Total pool space used           = 9500246016 (8.8G)
        Total pool preallocated         = 2579349504 (2.4G)
        Total pool snapshot space used  = 0
        Total pool non-base space used  = 0
        Health state                    = OK (5)
        Health details                  = "The LUN is operating
normally. No action is required."

5:      ID                              = res_3
        Name                            = CG1
        Resource type                   = LUN group
        Pool                            = pool_1
        Total pool space used           = 892542287872 (831.2G)
        Total pool preallocated         = 8863973376 (8.2G)
        Total pool snapshot space used  = 231799308288 (215.8G)
        Total pool non-base space used  = 231799308288 (215.8G)
        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 pool based on data access patterns.

The following table lists the attributes for FAST VP general settings.

Table 97 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:

Table 97 FAST VP general attributes (continued)

Attribute	Description
	`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.
`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 pool scheduled to be moved to a higher storage tier.
`Data to move down`	The amount of data in the pool scheduled to be moved to a lower storage tier.
`Data to move within`	The amount of data in the pool scheduled to be moved within the same storage tiers for rebalancing.
`Estimated scheduled 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. Valid values are: - `yes` - `no`

Qualifier	Description
`-schedEnabled`	Specify whether the pool is rebalanced according to the system FAST VP schedule. Valid values are: • `yes` • `no`
`-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 (supported physical deployments only)

FAST Cache is a storage efficiency technology that uses drives to expand the cache capability of the storage system to provide improved performance.

The following table lists the attributes for FAST Cache:

Table 98 FAST Cache attributes

Attribute	Description
`Capacity`	Capacity of the FAST Cache.
`Drives`	The list of drive types, and the number of drives of each type in the FAST Cache.
`Number of drives`	Total number of drives in the FAST Cache.
`RAID level`	RAID level applied to the FAST Cache drives. This value is always **RAID 1**.
`Health state`	Health state of the FAST Cache. The health state code appears in parentheses.

Table 98 FAST Cache attributes (continued)

Attribute	Description
`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 drive group to include in the FAST Cache. **Note** Only SAS Flash 2 drives can be used in the FAST Cache.
`-drivesNumber`	Specify the number of drives 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 drives from drive group dg_2, and enables FAST Cache on existing pools:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/
fastcache create -diskGroup dg_2 -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 for a medium endurance Flash drive:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/fastcache show -detail

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

1:     Total space           = 536870912000 (500G)
       Drives                = 6 x 200GB SAS Flash 2
       Number of drives      = 6
       RAID level            = 1
       Health state          = OK (5)
       Health details        = "The component is operating
normally.  No action is required."
```

Extend FAST Cache

Extend the FAST Cache by adding more drives.

Format

```
/stor/config/fastcache extend [-async] -diskGroup <value> -drivesNumber <value>
```

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.
-diskGroup	Specify the comma-separated list of SAS Flash drives to add to the FAST Cache. Any added drives must have the same drive type and drive size as the existing drives.
-drivesNumber	Specify the number of drives for each corresponding drive group to be added to the FAST Cache.

Example

The following command adds six drives from drive group "dg_2" to FAST cache.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/fastcache extend -diskGroup dg_2 -drivesNumber 6

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

Operation completed successfully.
```

Shrink FAST Cache

Shrink the FAST Cache by removing storage objects.

Format

```
/stor/config/fastcache shrink [-async] -so <value>
```

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-so`	Specify the comma-separated list of storage objects to remove from the FAST Cache. Run the `/stor/config/fastcache/so show` command to obtain a list of all storage objects currently in the FAST Cache.

Example

The following command removes Raid Group RG_1 from the FAST Cache.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/
fastcache shrink –so rg_1
```

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

Operation completed successfully.
```

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.
```

Manage FAST Cache storage objects (physical deployments only)

FAST Cache storage objects include the RAID groups and drives that are in the FAST Cache.

Table 99 FAST Cache storage object attributes

Attribute	Description
`ID`	Identifier of the storage object.
`Type`	Type of storage object.
`RAID level`	RAID level applied to the storage object.
`Drive type`	Type of drive.
`Number of drives`	Number of drives in the storage object.
`Drives`	Comma-separated list of the drive IDs for each storage object.
`Total space`	Total space used by the storage object.
`Device state`	The status of the FAST Cache device. Values are: • `OK` - This cache device is operating normally. • `Degraded` - One drive of this cache device is faulted. • `Faulted` - This cache device cannot operate normally. • `Expanding` - This cache device is expanding. • `Expansion Ready` - This cache device finished expanding. • `Expansion Failure` - This cache device failed to expand. • `Shrinking` - This cache device is shrinking. • `Shrink Done` - This cache device has flushed pages and is removed from FAST Cache.

View FAST Cache storage objects

View a list of all storage objects, including RAID groups and drives, that are in the FAST Cache.

Format

```
/stor/config/fastcache/so [-id <value> ] show
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the storage object in the FAST Cache.

Example 1

The following example shows FAST Cache storage objects on the system.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/
fastcache/so show
```

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

1:    ID                   = rg_6
      Type                 = RAID group
```

```
       Stripe length       = 2
       RAID level          = 1
       Number of drives    = 2
       Drive type          = SAS Flash 2
       Drives              = dae_0_1_disk_1, dae_0_1_disk_2
       Total space         = 195400433664 (181.9G)
       Device state        = OK
```

View storage profiles (physical deployments only)

Storage profiles are preconfigured settings for configuring pools based on the following:

- Types of storage resources that will use the pools.
- Intended usage of the pool.

For example, create a pool for file system storage resources intended for general use. When configuring a 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 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 100 Storage profile attributes

Attribute	Description
`ID`	ID of the storage profile.
`Type`	(Available only for systems that support dynamic pools) Type of pool the profile can create. Value is one of the following: • `Dynamic` • `Traditional`
`Description`	Brief description of the storage profile.
`Drive type`	Types of drives for the storage profile.
`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 drives the data is striped across.

Table 100 Storage profile attributes (continued)

Attribute	Description
	Note For best fit profiles, this value is `Best fit`.
`Disk group`	List of drive groups recommended for the storage pool configurations of the specified storage profile. This is calculated only when the `-configurable` option is specified.
`Maximum drives to configure`	List of the maximum number of drives allowed for the specified storage profile in the recommended drive groups. This is calculated only when the `-configurable` option is specified.
`Maximum capacity to configure`	List of the maximum number of free capacity of the drives available to configure for the storage profile in the recommended drive groups. This is calculated only when the `-configurable` option is specified.

Note

The show action command on page 23 explains how to change the output format.

Format

```
/stor/config/profile [-id <value> | -driveType <value> [-
raidLevel <value>] | -traditional] [-configurable] show
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of a storage profile.
`-driveType`	Specify the type of drive.
`-raidLevel`	Specify the RAID type of the profile.
`-traditional`	(Available only for systems that support dynamic pools) Specify this option to view the profiles that you can use for creating traditional pools. To view the profiles you can use for creating dynamic pools, omit this option.
`-configurable`	Show only profiles that can be configured, that is, those with non-empty drive group information. If specified, calculates the following drive group information for each profile: • `Disk group` • `Maximum drives to configure` • `Maximum capacity to configure` If the profile is for a dynamic pool, the calculated information indicates whether the drive group has enough drives for pool creation. The calculation assumes that the pool will be created with the drives in the specified drive group only.

Example 1

The following command shows details for storage profiles that can be used to create dynamic pools:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/profile -configurable show

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

1:    ID                            = profile_22
      Type                          = Dynamic
      Description                   = SAS Flash 2 RAID5 (4+1)
      Drive type                    = SAS Flash 2
      RAID level                    = 5
      Maximum capacity              = 4611148087296 (4.1T)
      Stripe length                 = Maximum capacity
      Disk group                    =
      Maximum drives to configure   =
      Maximum capacity to configure =

2:    ID                            = profile_30
      Type                          = Dynamic
      Description                   = SAS Flash 2 RAID10 (1+1)
      Drive type                    = SAS Flash 2
      RAID level                    = 10
      Maximum capacity              = 9749818597376 (8.8T)
      Stripe length                 = 2
      Disk group                    =
      Maximum drives to configure   =
      Maximum capacity to configure =

3:    ID                            = profile_31
      Type                          = Dynamic
      Description                   = SAS Flash 2 RAID10 (2+2)
      Drive type                    = SAS Flash 2
      RAID level                    = 10
      Maximum capacity              = 9749818597376 (8.8T)
      Stripe length                 = 4
      Disk group                    =
      Maximum drives to configure   =
      Maximum capacity to configure =
```

Example 2

The following command shows details for storage profiles that can be used to create traditional pools in models that support dynamic pools:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/profile -traditional -configurable show

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

1:    ID                            = tprofile_22
      Type                          = Traditional
      Description                   = SAS Flash 3 RAID5 (4+1)
      Drive type                    = SAS Flash 3
      RAID level                    = 5
      Maximum capacity              = 4611148087296 (4.1T)
      Stripe length                 = Maximum capacity
      Disk group                    = dg_16
      Maximum drives to configure   = 5
      Maximum capacity to configure = 1884243623936 (1.7T)

2:    ID                            = tprofile_30
      Type                          = Traditional
      Description                   = SAS Flash 3 RAID10 (1+1)
      Drive type                    = SAS Flash 3
      RAID level                    = 10
      Maximum capacity              = 9749818597376 (8.8T)
      Stripe length                 = 2
      Disk group                    = dg_13, dg_15
      Maximum drives to configure   = 10, 10
      Maximum capacity to configure = 1247522127872 (1.1T),
2954304921600 (2.6T)

3:    ID                            = tprofile_31
      Type                          = Traditional
      Description                   = SAS Flash 3 RAID10 (2+2)
      Drive type                    = SAS Flsh 3
      RAID level                    = 10
      Maximum capacity              = 9749818597376 (8.8T)
      Stripe length                 = 4
      Disk group                    = dg_13, dg_15
      Maximum drives to configure   = 8, 8
      Maximum capacity to configure = 2363443937280 (2.1T),
952103075840 (886.7G)
```

Manage drive groups (physical deployments only)

Drive groups are the groups of drives on the system with similar characteristics, including type, capacity, and spindle speed. When configuring pools, you select the drove group to use and the number of drives from the group to add to the pool.

Each drive group is identified by an ID.

The following table lists the attributes for drive groups.

Table 101 Drive group attributes

Attribute	Description
`ID`	ID of the drive group.
`Drive type`	Type of drives in the drive group.
`FAST Cache`	Indicates whether the drive group's drives can be added to FAST Cache.
`Drive size`	Capacity of one drive in the drive group.
`Rotational speed`	Rotational speed of the drives in the group.
`Number of drives`	Total number of drives in the drive group.
`Unconfigured drives`	Total number of drives in the drive group that are not in a pool.
`Capacity`	Total capacity of all drives in the drive group.
`Recommended number of spares`	Number of spares recommended for the drive group.
`Drives past EOL`	Number of drives past EOL (End of Life) in the group.

Table 101 Drive group attributes (continued)

Attribute	Description
`Drives approaching EOL`	Number of drives that will reach EOL in 0-30 days, 0-60 days, 0-90 days and 0-180 days.

View drive groups

View details about drive groups on the system. You can filter on the drive group ID.

Note

The show action command on page 23 explains how to change the output format.

Format

```
/stor/config/dg [-id <value>] [-traditional] show
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of a drive group.
`-traditional`	(Available only for systems that support dynamic pools) Specify this qualifier to have the system assume that the pools to be created are traditional pools.

Example 1

The following command shows details about all drive groups that can be used to configure dynamic pools:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/dg show
-detail
```

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

1:     ID                           = dg_3
       Drive type                   = SAS Flash 2
       FAST Cache                   = yes
       Drive size                   = 393846128640 (366.7G)
       Vendor size                  = 400.0G
       Rotational speed             = 0 rpm
       Number of drives             = 3
       Unconfigured drives          = 3
       Capacity                     = 1181538385920 (1.1T)
       Recommended number of spares = 0
       Drives past EOL              = 0
       Drives approaching EOL       = 0 (0-30 days), 0 (0-60 days),
0 (0-90 days), 0 (0-180 days)

2:     ID                           = dg_2
       Drive type                   = SAS Flash 2
       FAST Cache                   = yes
       Drive size                   = 196971960832 (183.4G)
       Vendor size                  = 200.0G
       Rotational speed             = 0 rpm
       Number of drives             = 7
       Unconfigured drives          = 7
       Capacity                     = 1378803725824 (1.2T)
       Recommended number of spares = 0
       Drives past EOL              = 0
       Drives approaching EOL       = 1 (0-30 days), 2 (0-60 days),
2 (0-90 days), 3 (0-180 days)
```

Example 2

The following command shows details about all drive groups that can be used to configure traditional pools in models that support dynamic pools:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/dg -traditional show
```

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

[Response]
Storage system address: 10.244.223.141
Storage system port: 443
HTTPS connection

1:     ID                           = dg_8
       Drive type                   = NL-SAS
       FAST Cache                   = no
       Drive size                   = 1969623564288 (1.7T)
       Vendor size                  = 2.0T
       Rotational speed             = 7200 rpm
       Number of drives             = 7
       Unconfigured drives          = 7
       Capacity                     = 13787364950016 (12.5T)
       Recommended number of spares = 1

2:     ID                           = dg_15
       Drive type                   = SAS
       FAST Cache                   = no
       Drive size                   = 590894538752 (550.3G)
       Vendor size                  = 600.0G
       Rotational speed             = 15000 rpm
       Number of drives             = 16
       Unconfigured drives          = 4
       Capacity                     = 9454312620032 (8.5T)
       Recommended number of spares = 1
```

View recommended drive group configurations

View the recommended drive groups from which to add drives to a pool based on a specified storage profile or pool type.

Note

The show action command on page 23 explains how to change the output format.

Format

```
/stor/config/dg recom {-profile <value>| -pool <value> | -poolName <value>}
```

Action qualifier

Qualifier	Description
`-profile`	Type the ID of a storage profile. The output will include the list of drive groups recommended for the specified storage profile.
`-pool`	Type the ID of a pool. The output will include the list of drive groups recommended for the specified pool.
`-poolName`	Type the name of a pool. The output will include the list of drive groups recommended for the specified pool.

Example

The following command shows the recommended drive groups for pool pool_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/dg
recom -pool pool_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 storage system capacity settings

The following table lists the general storage system capacity attributes:

Table 102 General storage system capacity attributes

Attributes	Description
`Free space`	Specifies the amount of space that is free (available to be used) in all storage pools on the storage system.
`Used space`	Specifies the amount of space that is used in all storage pools on the storage system.
`Total space`	Specifies the total amount of space, both free and used, in all storage pools on the storage system.
`Data Reduction space saved`	Specifies the storage size saved on the entire system when using data reduction.

Table 102 General storage system capacity attributes (continued)

Attributes	Description
	Note Data reduction is available for thin LUNs and thin file systems in an All-Flash pool only. The thin file systems must be created on Unity systems running version 4.2.x or later.
`Data Reduction percent`	Specifies the storage percentage saved on the entire system when using data reduction. Note Data reduction is available for thin LUNs and thin file systems in an All-Flash pool only. The thin file systems must be created on Unity systems running version 4.2.x or later.
`Data Reduction ratio`	Specifies the ratio between data without data reduction and data after data reduction savings. Note Data reduction is available for thin LUNs and thin file systems in an All-Flash pool only. The thin file systems must be created on Unity systems running version 4.2.x or later.

View system capacity settings

View the current storage system capacity settings.

Format

```
/stor/general/system show
```

Example

The following command displays details about the storage capacity on the system:

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

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

1:      Free space                          = 4947802324992 (1.5T)
        Used space                          = 4947802324992 (1.5T)
        Total space                         = 9895604649984 (3.0T)
        Compression space saved             = 4947802324992 (1.5T)
        Compression percent                 = 50%
        Compression ratio                   = 1
        Data Reduction space saved          = 4947802324992 (1.5T)
        Data Reduction percent              = 50%
        Data Reduction ratio                = 1
```

Manage system tier capacity settings

The following table lists the general system tier capacity attributes:

Table 103 General system tier capacity attributes

Attributes	Description
`Name`	Name of the tier. One of the following: • Extreme Performance • Performance • Capacity
`Free space`	Specifies the amount of space that is free (available to be used) in the tier.
`Used space`	Specifies the amount of space that is used in the tier.
`Total space`	Specifies the total amount of space, both free and used, in the tier.

View system tier capacity

View the current system tier capacity settings.

Format

```
/stor/general/tier show
```

Example

The following command displays details about the storage tier capacity on the system:

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

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

1:      Name        = Extreme Performance Tier
        Free space  = 4947802324992 (1.5T)
        Used space  = 4947802324992 (1.5T)
        Total space = 9895604649984 (3.0T)

2:      Name        = Capacity Tier
        Free space  = 4947802324992 (1.5T)
        Used space  = 4947802324992 (1.5T)
        Total space = 9895604649984 (3.0T)
```

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:

- SMB shares (previously named CIFS shares), which provide storage access to Windows hosts.
- Network file system (NFS) shares, which provide storage access to Linux/UNIX hosts.

An ID identifies each file system.

The following table lists the attributes for file systems:

Table 104 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. • `OK_BUT (7)`—File system is working, but one or more of the following may have occurred: ■ The storage resource is being initialized or deleted. ■ The file system on this storage resource is running out of space. Allocate more storage space to the storage resource. • `Degraded/Warning (10)`—Working, but one or more of the following may have occurred: ■ One or more of its storage pools are degraded. ■ A replication session for the storage resource is degraded. ■ It has almost reached full capacity. Increase the primary storage size, or create additional file systems to store the data, to avoid data loss. Change file system settings on page 401 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. • `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 the data, to avoid data loss. Change file system settings on page 401 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.

Table 104 File system attributes (continued)

Attribute	Description
	■ 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 displays only the file system ID. This enables you to easily identify the file system in the output.
`Server`	Name of the NAS server that the file system is mounted on.
`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.
`Format`	Format of the file system. Value is `UFS64`.
`Protocol`	Protocol used to enable network shares from the file system. Value is one of the following: • `nfs`—Protocol for Linux/UNIX hosts. • `cifs`—Protocol for Windows hosts. • `multiprotocol`—Protocol for UNIX and Windows hosts.
`Access policy`	(Applies to multiprotocol file systems only.) File system access policy option. Value is 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 that are defined in Windows ACLs are honored for both Windows and UNIX/Linux clients (UNIX mode bits are ignored).
`Folder rename policy`	(Applies to multiprotocol file systems only.) File system folder rename policy option. This policy controls the circumstances under which NFS and SMB clients can rename a directory. Value is one of the following: • `forbiddenSmb` (default)—Only NFS clients can rename directories without any restrictions. An SMB client cannot rename a directory if at least one file is opened in the directory or in one of its subdirectories. • `allowedAll` —All NFS and SMB clients can rename directories without any restrictions. • `forbiddenAll`—NFS and SMB clients cannot rename a directory if at least one file is opened in the directory or in one of its subdirectories.

Table 104 File system attributes (continued)

Attribute	Description
`Locking policy`	(Applies to multiprotocol file systems only.) File system locking policy option. This policy controls whether NFSv4 range locks must be honored. Value is one of the following: - `mandatory` (default)—Uses the SMB and NFSv4 protocols to manage range locks for a file that is in use by another user. A mandatory locking policy prevents data corruption if there is concurrent access to the same locked data. - `advisory` —In response to lock requests, reports that there is a range lock conflict, but does not prevent the access to the file. This policy allows NFSv2 and NFSv3 applications that are not range-lock-compliant to continue working, but risks data corruption if there are concurrent writes.
`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`	Identifies 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.
`Data Reduction enabled`	Identifies whether data reduction is enabled for this file system. Valid values are: - `yes` - `no` (default) **Note** Data reduction is available for thin file systems in an All-Flash pool only. The thin file systems must be created on Unity systems running version 4.2.x or later.
`Data Reduction space saved`	Total space saved (in gigabytes) for this file system by using data reduction.

Table 104 File system attributes (continued)

Attribute	Description
	Note Data reduction is available for thin file systems in an All-Flash pool only. The thin file systems must be created on Unity systems running version 4.2.x or later.
`Data Reduction percent`	Total file system storage percentage saved for the file system by using data reduction. **Note** Data reduction is available for thin file systems in an All-Flash pool only. The thin file systems must be created on Unity systems running version 4.2.x or later.
`Data Reduction ratio`	Ratio between data without data reduction and data after data reduction savings. **Note** Data reduction is available for thin file systems in an All-Flash pool only. The thin file systems must be created on Unity systems running version 4.2.x or later.
`Advanced deduplication enabled`	Identifies whether advanced deduplication is enabled for this file system. This option is available only after data reduction has been enabled. An empty value indicates that advanced deduplication is not supported on the file system. Valid values are: • `yes` • `no` (default) **Note** The thin file systems must be created on a Unity system running version 4.2.x or later. Advanced deduplication is available on Unity All-Flash 450F, 550F, and 650F systems only.
`Current allocation`	If enabled, the quantity of primary storage currently allocated through thin provisioning.
`Total pool space preallocated`	Space reserved from the pool for the file system for future needs to make writes more efficient. The pool may be able to reclaim some of this space if pool space is low.
`Total pool space used`	Total pool space used in the pool for the file system. This includes the allocated space and allocations for snaps and overhead. This does not include preallocated space.
`Minimum size allocated`	(Displays for file systems created on a Unity system running OE version 4.1.) Minimum quantity of primary storage allocated through thin provisioning. File shrink operations cannot decrease the file system size lower than this value.

Table 104 File system attributes (continued)

Attribute	Description
`Protection size used`	Quantity of storage currently used for protection data.
`Protection schedule`	ID of an applied protection schedule. View protection schedules on page 106 explains how to view the IDs of schedules on the system.
`Protection schedule paused`	Identifies whether an applied protection schedule is currently paused. Value is yes or no.
`FAST VP policy`	FAST VP tiering policy for the file system. This policy defines both the initial tier placement and the ongoing automated tiering of data during data relocation operations. Valid values (case-insensitive): • `startHighThenAuto` (default)—Sets the initial data placement to the highest-performing drives with available space, and then relocates portions of the storage resource's data based on I/O activity. • `auto`—Sets the initial data placement to an optimum, system-determined setting, and then relocates portions of the storage resource's data based on the storage resource's performance statistics such that data is relocated among tiers according to I/O activity. • `highest`—Sets the initial data placement and subsequent data relocation (if applicable) to the highest-performing drives with available space. • `lowest`—Sets the initial data placement and subsequent data relocation (if applicable) to the most cost-effective drives with available space.
`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. • `<value>` is the percentage of storage in that tier.
`CIFS synchronous write`	Identifies whether SMB synchronous writes option is enabled. Value is `yes` or `no`. • The SMB synchronous writes option provides enhanced support for applications that store and access database files on Windows network shares. On most SMB filesystems read operations are synchronous and write operations are asynchronous. When you enable the SMB synchronous writes option for a Windows (SMB) file system, the system performs immediate synchronous writes for storage operations, regardless of how the SMB protocol performs write operations. • Enabling synchronous write operations allows you to store and access database files (for example, MySQL) on SMB network shares. This option guarantees that any write to the share is

Table 104 File system attributes (continued)

Attribute	Description
	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 SMB 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 SMB synchronous write.
`CIFS oplocks`	Identifies whether opportunistic file locks (oplocks) for SMB network shares are enabled. Value is `yes` or `no`. • Oplocks allow SMB clients to buffer file data locally before sending it to a server. SMB 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 (SMB) 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`	Identifies whether write notifications for SMB 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 SMB share. **Note** If this option is enabled, the value for SMB directory depth indicates the lowest directory level to which the notification setting applies.
`CIFS notify on access`	Identifies whether file access notifications for SMB shares are enabled. Value is `yes` or `no`. When enabled, Windows applications receive notifications each time a user accesses a file on the SMB share. **Note** If this option is enabled, the value for SMB directory depth indicates the lowest directory level to which the notification setting applies.
`CIFS directory depth`	For write and access notifications on SMB network shares, the subdirectory depth permitted for file notifications. Value range is 1-512. Default is 512.

Table 104 File system attributes (continued)

Attribute	Description
`Replication type`	Identifies what type of asynchronous replication this file system is participating in. Valid values are: • `none` • `local` • `remote`
`Synchronous replication type`	Identifies what type of synchronous replication this file system is participating in. Valid values are: • `none` • `remote`
`Replication destination`	Identifies whether the storage resource is a destination for a replication session (local or remote). Valid values are: • `yes` • `no`
`Migration destination`	Identifies whether the storage resource is a destination for a NAS import session. Valid values are: • `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.
`Pool full policy`	Policy to follow when the pool is full and a write to the file system is attempted. This attribute enables you to preserve snapshots on the file system when a pool is full. Valid values are: • `Delete All Snaps` (default for thick file systems)—Delete snapshots associated with the file system when the pool reaches full capacity. • `Fail Writes` (default for thin file systems)—Fail write operations to the file system when the pool reaches full capacity. **Note** This attribute is only available for existing file systems. You cannot specify this attribute when creating a file system.
`Event publishing protocols`	List of file system access protocols enabled for Events Publishing. By default, the list is empty. Valid values are: • `nfs`—Enable Events Publishing for NFS. • `cifs`—Enable Events Publishing for SMB (CIFS).

Table 104 File system attributes (continued)

Attribute	Description
`FLR mode`	Specifies which verison of File-level Retention (FLR) is enabled. Values are: • `enterprise` • `compliance` • `disabled`
`FLR has protected files`	Indicates whether the file system contains protected files. Values are: • `yes` • `no`
`FLR clock time`	Indicates file system clock time to track the retention date. For example, `2019-02-20 12:55:32`.
`FLR max retention date`	Maximum date and time that has been set on any locked file in an FLR-enabled file system. `2020-09-20 11:00:00`
`FLR min retention period`	Indicates the shortest retention period for which files on an FLR-enabled file system can be locked and protected from deletion. The format is `(<integer> d|m|y) | infinite`. Values are: • `d: days` • `m: months` • `y: years` (default is 1 day `1d`) • `infinite` Any non-infinite values plus the current date must be less than the maximum retention period of 2106-Feb-07.
`FLR default retention period`	Indicates the default retention period that is used in an FLR-enabled file system when a file is locked and a retention period is not specified at the file level. The format is `(<integer> d|m|y) | infinite`. Values are: • `d: days` • `m: months` • `y: years` (FLR-C `compliance` default is 1 year--`1y`) • `infinite` (FLR-E `enterprise` default) Any non-infinite values plus the current date must be less than the maximum retention period of 2106-Feb-07.
`FLR max retention period`	Indicates the longest retention period for which files on an FLR-enabled file system can be locked and protected from deletion. Values are: • `d: days` • `m: months` • `y: years`

Table 104 File system attributes (continued)

Attribute	Description
	- `infinite` (default) The value should be greater than 1 day. Any non-infinite values plus the current date must be less than the maximum retention period of 2106-Feb-07.
`FLR auto lock enabled`	Indicates whether automatic file locking for all files in an FLR-enabled file system is enable. Values are: - `yes` - `no`
`FLR auto delete enabled`	Indicates whether automatic deletion of locked files from an FLR-enabled file system once the retention period has expired is enabled. Values are: - `yes` - `no` **Note** The system scans for expired files every seven days and deletes them automatically if auto-delete is enabled. The seven day period begins the day after auto-delete is enabled on the file system.
`FLR policy interval`	When Auto-lock new files is enabled, this indicates a time interval for how long to wait after files are modified before the files are automatically locked in an FLR-enabled file system. The format is *<value>*`<qualifier>`, where value is an integer and the qualifier is: - `m`--minutes - `h`--hours - `d`--days The value should be greater than 1 minute and less than 366 days.

Create file systems

Create a multiprotocol file system, NFS file system, or CIFS (SMB) 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 the file system to associate it with a share.

Note

Size qualifiers on page 22 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 drive to the pool. Configure custom pools on page 344 explains how to create custom pools.
- Configure at least one NAS server to which to associate the file system. Create a NAS server on page 126 explains how to configure NAS servers.

Format

```
/stor/prov/fs create [-async] -name <value> [-descr <value>] {-
server <value> | -serverName <value>} {-pool <value> | -
poolName <value>} -size <value> [-thin {yes | no}] [-
dataReduction {yes [-advancedDedup {yes | no}] | no}] [-
minSizeAllocated <value>] -type {{nfs | cifs | multiprotocol [-
accessPolicy {native | Windows | Unix}] [-folderRenamePolicy
{allowedAll | forbiddenSmb | forbiddenAll}] [-lockingPolicy
{advisory | mandatory}]} [-cifsSyncWrites {yes | no}] [-
cifsOpLocks {yes | no}] [-cifsNotifyOnWrite {yes | no}] [-
cifsNotifyOnAccess {yes | no}] [-cifsNotifyDirDepth <value>] |
nfs} [-fastvpPolicy {startHighThenAuto | auto | highest |
lowest}] [-sched <value> [-schedPaused {yes | no}]] [-replDest
{yes | no}][-eventProtocols <value>] [-flr {disabled |
{enterprise | compliance} [-flrMinRet <value>] [-flrDefRet
<value>] [-flrMaxRet <value>]}}
```

Action qualifiers

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 parent NAS server for the file system. View NAS servers on page 128 explains how to view the IDs of the NAS servers on the system.
`-serverName`	Type the name of the NAS server that will be the parent NAS server for the file system.
`-pool`	Type the ID of the pool to be used for the file system.
`-poolName`	Type the name of the pool to be used for the file system. This value is case insensitive. View pools on page 355 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.
`-thin`	Enable thin provisioning on the file system. Valid values are: • `yes` (default) • `no`

Qualifier	Description
-dataReduction	Specify whether data reduction is enabled for the thin file system. Valid values are: • yes (default) • no **Note** Data reduction is available for thin file systems in an All-Flash pool only. The thin file systems must be created on Unity systems running version 4.2.x or later.
-advancedDedup	Specify whether advanced deduplication is enabled for the thin file system. This option is available only after data reduction has been enabled. Valid values are: • yes • no (default) **Note** The thin file systems must be created on a Unity system running version 4.2.x or later. Advanced deduplication is available on Unity All-Flash 450F, 550F, and 650F systems only.
-minSizeAllocated	(Option available on a Unity system running OE version 4.1.) Specify the minimum size to allocate for the thin file system. Automatic and manual file shrink operations cannot decrease the file system size lower than this value. The default value is 3G, which is the minimum thin file system size.
-type	Specify the type of network shares to export from the file system. Valid values are: • nfs — Network shares for Linux/UNIX hosts. • cifs — Network shares for Windows hosts. • multiprotocol — Network shares for multiprotocol sharing.
-accessPolicy	(Applies to multiprotocol file systems only.) Specify the access policy for this file system. Valid values are: • native (default) • unix • windows
-folderRenamePolicy	(Applies to multiprotocol file systems only.) Specify the rename policy for the file system. Valid values are: • forbiddenSMB (default) • allowedAll

Qualifier	Description
	- `forbiddenAll`
`-lockingPolicy`	(Applies to multiprotocol file systems only.) Specify the locking policy for the file system. Valid values are: - `mandatory` (default) - `advisory`
`-cifsSyncWrites`	Enable synchronous write operations for CIFS network shares. Valid values are: - `yes` - `no` (default)
`-cifsOpLocks`	Enable opportunistic file locks (oplocks) for CIFS network shares. Valid values are: - `yes` (default) - `no`
`-cifsNotifyOnWrite`	Enable to receive notifications when users write to a CIFS share. Valid values are: - `yes` - `no` (default)
`-cifsNotifyOnAccess`	Enable to receive notifications when users access a CIFS share. Valid values are: - `yes` - `no` (default)
`-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.
`-folderRenamePolicy`	Specify to rename the policy type for the specified file system. Valid values are: - `allowedAll` - `forbiddenSmb` (default) - `forbiddenAll`
`-lockingPolicy`	Set the locking policy for this type of file system. Valid values are: - `advisory` - `mandatory` (default)
`-fastvpPolicy`	Specify the FAST VP tiering policy for the file system. This policy defines both the initial tier placement and the ongoing automated tiering of data during data relocation operations. Valid values (case insensitive):

Qualifier	Description
	• `startHighThenAuto` (default) — Sets the initial data placement to the highest-performing drives with available space, and then relocates portions of the storage resource's data based on I/O activity. • `auto` — Sets the initial data placement to an optimum, system-determined setting, and then relocates portions of the storage resource's data based on the storage resource's performance statistics such that data is relocated among tiers according to I/O activity. • `highest` — Sets the initial data placement and subsequent data relocation (if applicable) to the highest-performing drives with available space. • `lowest` — Sets the initial data placement and subsequent data relocation (if applicable) to the most cost-effective drives with available space.
`-sched`	Type the ID of a protection schedule to apply to the storage resource. View protection schedules on page 106 explains how to view the IDs of the schedules on the system.
`-schedPaused`	Specify whether to pause the protection schedule specified for `-sched`. Valid values are: • `yes` • `no`
`-replDest`	Specifies whether the resource is a replication destination. Valid values are: • `yes` • `no` (default)
`-eventProtocols`	Specifies the comma-separated list of file system access protocols enabled for Events Publishing. By default, the list is empty. Valid values are: • `nfs` — Enable Events Publishing for NFS. • `cifs` — Enable Events Publishing for CIFS (SMB).
`-flr`	Specifies whether File-level Retention (FLR) is enabled and if so, which version of FLR is being used. Valid values are: • `enterprise` — Specify to enable FLR-E. • `compliance` — Specify to enable FLR-C. • `disabled` (default) — Specify to disable FLR.
`-flrMinRet`	Specify the shortest retention period for which files on an FLR-enabled file system will be locked and protected from deletion. Valid values are:

Qualifier	Description
	• `d: days` (default is 1 day `1d`) • `m: months` • `y: years` • `infinite`
`-flrDefRet`	Specify the default retention period that is used in an FLR-enabled file system where a file is locked, but a retention period was not specified at the file level. The format is `(<integer> d|m|y) | infinite`. • `d: days` • `m: months` • `y: years` — FLR-C (`compliance`) default is 1 year--`1y`) • `infinite` — FLR-E (`enterprise`) default Any non-infinite values plus the current date must be less than the maximum retention period of 2106-Feb-07. The value of this parameter must be greater than the minimum retention period `-flrMinRet`.
`-flrMaxRet`	Specify the maximum date and time that has been set on any locked file in an FLR-enabled file system. Values are: • `d: days` • `m: months` • `y: years` • `infinite` (default) The value should be greater than 1 day. Any non-infinite values plus the current date must be less than the maximum retention period of 2106-Feb-07. The value of this parameter must be greater than the default retention period `-flrDefRet`.

Example

The following command creates a file system with these settings:

- Name is FileSystem01.
- Description is "Multiprotocol file system".
- Uses the capacity storage pool.
- Uses NAS server nas_2 as the parent NAS server.
- Primary storage size is 3 GB.
- Supports multiprotocol network shares.
- Has a native access policy.
- Is a replication destination.

The file system receives the ID res_28:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs create
-name FileSystem01 -descr "Multiprotocol file system" -server nas_2 -
```

```
pool capacity -size 3G -type multiprotocol -accessPolicy native -
replDest yes
```

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

ID = res_28
Operation completed successfully.
```

View file systems

View details about a file system. You can filter on the file system ID.

Note

The show action command on page 23 explains how to change the output format.

Format

```
/stor/prov/fs [{-id <value> | -name <value> | -server <value> |
-serverName <value>}] show
```

Object qualifiers

Qualifier	Description
`-id`	Type the ID of a file system.
`-name`	Type the name of a file system.
`-server`	Type the ID of the NAS server for which the file systems will be displayed.
`-serverName`	Type the name of the NAS server for which the file systems will be displayed.

Example

The following command lists details about all file systems on the storage system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs show -
detail
```

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

1:     ID                              = SF_1
       Name                            = MyFS
       Description                     = my file system
       Health state                    = OK (5)
       Health details                  = "The component is operating
normally. No action is required."
       File system                     = fs_1
       Server                          = SFS_1
       Storage pool ID                 = pool_1
       Storage pool                    = Performance
       Format                          = UFS64
       Protocol                        = nfs
       Access policy                   = native
       Folder rename policy            = allowedAll
       Locking policy                  = advisory
       Size                           = 107374182400 (100.0G)
       Size used                      = 1620303872 (1.5G)
       Maximum size                   = 281474976710656 (256.0T)
       Thin provisioning enabled      = yes
       Compression enabled            = no
       Compression space saved        = 0
       Compression percent            = 0%
       Compression ratio              = 1.0:1
       Data Reduction enabled         = no
       Data Reduction space saved     = 0
       Data Reduction percent         = 0%
       Data Reduction ratio           = 1.0:1
       Advanced deduplication enabled = no
       Current allocation             = 283140096 (270.0M)
       Preallocated                   = 2401214464 (2.2G)
       Total Pool Space Used          = 4041236480 (3.7G)
       Minimum size allocated         =
       Protection size used           = 0
       Snapshot count                 = 0
       Protection schedule            =
       Protection schedule paused     = no
       FLR mode                       = Disabled
       FLR has protected files        =
       FLR clock time                 =
       FLR max retention date         =
       FLR min retention period       =
       FLR default retention period   =
       FLR max retention period       =
       FLR auto lock enabled          =
       FLR auto delete enabled        =
       FLR policy interval            =
       CIFS synchronous write         = no
       CIFS oplocks                   = yes
       CIFS notify on write           = no
       CIFS notify on access          = no
       CIFS directory depth           = 512
       Replication type               = none
       Synchronous replication type   = none
       Replication destination        = no
       Migration destination          = no
       FAST VP policy                 = Start high then auto-tier
       FAST VP distribution           = Extreme Performance: 0%,
Performance: 100%, Capacity: 0%
       Creation time                  = 2018-09-21 14:44:31
       Last modified time             = 2018-09-21 14:44:31
       Pool full policy               = Fail Writes
       Event publishing protocols     =
```

Change file system settings

Change the settings for a file system.

Note

Size qualifiers on page 22 explains how to use the size qualifiers when specifying a storage size.

Format

/stor/prov/fs {-id *<value>* | -name *<value>*} set [-async] [-descr *<value>*] [-accessPolicy {native | Unix | Windows}] [-folderRenamePolicy {allowedAll | forbiddenSmb | forbiddenAll}] [-lockingPolicy {advisory | mandatory}] [-size *<value>*] [-minSizeAllocated *<value>*] [-dataReduction {yes [-advancedDedup {yes | no}] | 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}] [-
replDest {yes | no}] [-poolFullPolicy {deleteAllSnaps |
failWrites}] [-eventProtocols <value>] [-flr [-flrMinRet
<value>] [-flrDefRet <value>] [-flrMaxRet <value>] [-
flrAutoLock { yes | no}] [-flrAutoDelete {yes | no }] [-
flrPolicyInterval <value>]]
```

Object qualifiers

Qualifier	Description
-id	Type the ID of the file system to change.
-name	Type the name of the file system to change.

Action qualifiers

Qualifier	Description
-async	Run the operation in asynchronous mode.
-descr	Type a brief description of the file system.
-accessPolicy	(Applies to multiprotocol file systems only.) Specify the access policy for the file system. Valid values are: • native • unix • windows
-folderRenamePolicy	(Applies to multiprotocol file systems only.) Specify the rename policy for the file system. Valid values are: • forbiddenSMB (default) • allowedAll • forbiddenAll
-lockingPolicy	(Applies to multiprotocol file systems only.) Specify the locking policy for the file system. Valid values are: • mandatory (default) • advisory
-size	Type the amount of storage in the pool to reserve for the file system.
-minSizeAllocated	(Option available on a Unity system running OE version 4.1.) Specify the minimum size to allocate for the thin file system. Automatic and manual file shrink operations cannot decrease the file system size lower than this value. The default value is 3G, which is the minimum thin file system size.
-dataReduction	Enable data reduction on the thin file system. Valid values are:

Qualifier	Description
	- yes - no **Note** Data reduction is available for thin file systems in an All-Flash pool only. The thin file systems must have been created on Unity systems running version 4.2.x or later.
-advancedDedup	Enable advanced deduplication on the thin file system. This option is available only after data reduction has been enabled. Valid values are: - yes - no (default) **Note** The thin file systems must be created on a Unity system running version 4.2.x or later. Advanced deduplication is available on Unity All-Flash 450F, 550F, and 650F systems only.
-cifsSyncWrites	Enable synchronous write operations for CIFS (SMB) network shares. Valid values are: - yes - no
-cifsOpLocks	Enable opportunistic file locks (oplocks) for CIFS network shares. Valid values are: - yes - no
-cifsNotifyOnWrite	Enable to receive notifications when users write to a CIFS share. Valid values are: - yes - no
-cifsNotifyOnAccess	Enable to receive notifications when users access a CIFS share. Valid values are: - yes - 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 106 explains how to view the IDs of the schedules on the system.

Qualifier	Description
`-schedPaused`	Pause the schedule specified for the `-sched` qualifier. Valid values are: • `yes` • `no`
`-noSched`	Unassigns the protection schedule.
`-fastvpPolicy`	Specify the FAST VP tiering policy for the file system. This policy defines both the initial tier placement and the ongoing automated tiering of data during data relocation operations. Valid values (case-insensitive): • `startHighThenAuto` (default)—Sets the initial data placement to the highest-performing drives with available space, and then relocates portions of the storage resource's data based on I/O activity. • `auto`—Sets the initial data placement to an optimum, system-determined setting, and then relocates portions of the storage resource's data based on the storage resource's performance statistics such that data is relocated among tiers according to I/O activity. • `highest`—Sets the initial data placement and subsequent data relocation (if applicable) to the highest-performing drives with available space. • `lowest`—Sets the initial data placement and subsequent data relocation (if applicable) to the most cost-effective drives with available space.
`-replDest`	Specifies whether the resource is a replication destination. Valid values are: • `yes` • `no`
`-poolFullPolicy`	Specifies the policy to follow when the pool is full and a write to the file system is tried. This attribute enables you to preserve snapshots on the file system when a pool is full. Valid values are: • `deleteAllSnaps`—Delete snapshots that are associated with the file system when the pool reaches full capacity. • `failWrites`—Fail write operations to the file system when the pool reaches full capacity.
`-eventProtocols`	Specifies a list of file system access protocols enabled for Events Publishing. By default, the list is empty. Valid values are: • `nfs`—Enable Events Publishing for NFS. • `cifs`—Enable Events Publishing for CIFS (SMB).

Qualifier	Description
-flrMinRet	Specify the shortest retention period for which files on an FLR-enabled file system will be locked and protected from deletion. Valid values are: • d: days (default is 1 day 1d) • m: months • y: years • infinite
-flrDefRet	Specify the default retention period that is used in an FLR-enabled file system where a file is locked, but a retention period was not specified at the file level. The format is (<integer> d|m|y) | infinite. • d: days • m: months • y: years — FLR-C (compliance) default is 1 year--1y) • infinite — FLR-E (enterprise) default Any non-infinite values plus the current date must be less than the maximum retention period of 2106-Feb-07. The value of this parameter must be greater than the minimum retention period -flrMinRet.
-flrMaxRet	Specify the maximum date and time that has been set on any locked file in an FLR-enabled file system. Values are: • d: days • m: months • y: years • infinite (default) The value should be greater than 1 day. Any non-infinite values plus the current date must be less than the maximum retention period of 2106-Feb-07. The value of this parameter must be greater than the default retention period -flrDefRet.
-flrAutoLock	Specify whether automatic file locking is enabled for all new files in an FLR-enabled file system. Valid values are: • yes • no
-flrAutoDelete	Specify whether locked files in an FLR-enabled file system will automatically be deleted once the retention period expires. Valid values are: • yes • no

Qualifier	Description
`-flrPolicyInterval`	If `-flrAutoLock` is set to `yes`, specify a time interval for how long after files are modified they will be automatically locked in an FLR-enabled file system. The format is *<value>*`<qualifier>`, where value is an integer and the qualifier is: • `m`--minutes • `h`--hours • `d`--days The value should be greater than 1 minute and less than 366 days.

Example

The following command specifies Events Publishing protocols:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs -id res_1 set -eventProtocols nfs,cifs`

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

ID = res_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 storage system.

Note

You cannot delete an FLR-C enabled file system that has currently locked and protected files. An FLR-E file system can be deleted, even if it does contain protected files.

Format

```
/stor/prov/fs {-id <value> | -name <value>} delete [-deleteSnapshots {yes | no}] [-async]
```

Object qualifiers

Qualifier	Description
`-id`	Type the ID of the file system to delete.
`-name`	Type the name of the file system to delete.

Action qualifiers

Qualifier	Description
`-deleteSnapshots`	Specifies that snapshots of the file system can be deleted along with the file system itself. Valid values are: • `yes` • `no` (default)
`-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 res_1 delete`

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

Operation completed successfully.
```

Manage user quotas for file systems and quota trees

A user quota limits the amount of storage consumed by an individual user storing data on a file system or quota tree.

The following table lists the attributes for user quotas:

Table 105 Attributes for user quotas

Attribute	Description
`File system`	Identifier for the file system that the quota will act upon. The file system cannot be read-only or a replication destination.
`Path`	Quota tree path relative to the root of the file system. If the user quota is on a file system, either do not use this qualifier, or set its value to `/`.
`User ID`	User identifier on the file system.
`Unix name`	Comma-separated list of Unix user names associated with the user quota. Multiple Unix names may appear when the file system is a multiple protocol file system and multiple Unix names map to one Windows name in the user mapping configuration file (nxtmap).
`Windows SIDs`	Comma-separated list of Windows SIDs associated with the user quota. **Note** The number of displayed SIDs is limited to 16. If the number of SIDs is over 16, only first 16 are displayed.

Table 105 Attributes for user quotas (continued)

Attribute	Description
`Windows name`	Comma-separated list of Windows user names associated with the user quota. Multiple Windows names may appear when the file system is a multiple protocol file system and multiple Windows names map to one Unix name in the user mapping configuration file (nxtmap). **Note** If the number of Windows names is over 16, only the first 16 Windows names are displayed.
`Space used`	Spaced used on the file system or quota tree by the specified user.
`Soft limit`	Preferred limit on storage usage. The system issues a warning when the soft limit is reached.
`Hard limit`	Absolute limit on storage usage. If the hard limit is reached for a user quota on a file system or quota tree, the user will not be able to write data to the file system or tree until more space becomes available.
`Grace period left`	Time period for which the system counts down days once the soft limit is met. If the user's grace period expires, users cannot write to the file system or quota tree until more space becomes available, even if the hard limit has not been reached.
`State`	State of the user quota. Valid values are: • `OK` • `Soft limit exceeded` • `Soft limit exceeded and grace period expired` • `Hard limit exceeded`

Create a user quota on a file system or quota tree

You can create user quotas on a file system or quota tree:

- Create a user quota on a file system to limit or track the amount of storage space that an individual user consumes on that file system. When you create or modify a user quota on a file system, you have the option to use default hard and soft limits that are set at the file-system level.
- Create a user quota on a quota tree to limit or track the amount of storage space that an individual user consumes on that tree. When you create a user quota on a quota tree, you have the option to use the default hard and soft limits that are set at the quota-tree level.

Format

```
/quota/user create [-async] {-fs <value> | -fsName <value>} [-
path <value>] {-userId <value> | -unixName <value> | -winName
<value>} {-default | [-softLimit <value>] [-hardLimit <value>]}
```

Action qualifiers

Qualifier	Description
-async	Run the operation in asynchronous mode.
-fs	Specify the ID of the file system that the quota will act upon. The file system cannot be read-only or a replication destination.
-fsName	Specify the name of the file system that the quota will act upon. The file system cannot be read-only or a replication destination.
-path	Specify either of the following: • If the user quota is for a file system, either do not use this qualifier, or set its value to /. • If the user quota is for a quota tree, specify the quota tree path relative to the root of the file system.
-userId	Specify the user ID on the file system or quota tree.
-unixName	Specify the UNIX user name associated with the specified user ID.
-winName	Specify the Windows user name associated with the specified user ID. The format is: [<domain>\]<name>
-default	Inherit the default quota limit settings for the user. To view the default limits, use the following command: /quota/config -fs *<value>* -path *<value>* show If a soft limit or hard limit has not been specified for the user, the default limit is applied.
-softLimit	Specify the preferred limit on storage usage by the user. A value of 0 means no limitation. If the hard limit is specified and the soft limit is not specified, there will be no soft limitation.
-hardLimit	Specify the absolute limit on storage usage by the user. A value of 0 means no limitation. If the soft limit is specified and the hard limit is not specified, there will be no hard limitation. **Note** The hard limit should be larger than the soft limit.

Example

The following command creates a user quota for user 201 on file system res_1, quota tree /qtree_1. The new user quota has the following limits:

- Soft limit is 20 GB.
- Hard limit is 50 GB.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /quota/user create -
fs res_1 -path /qtree_1 -userId 201 -softLimit 20G -hardLimit 50G
```

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

```
Operation completed successfully.
```

View user quotas

You can display space usage and limit information for user quotas on a file system or quota tree.

Because there can be a large amount of user quotas on a file system or quota tree, to reduce the impact on system performance, the system only updates user quota data every 24 hours. You can use the refresh action to update the data more often. Use the `/quota/config show` command to see the time spent for the data refresh.

Note

The Unix name and Windows name values are returned only when displaying a single user quota.

Note

The show action command on page 23 explains how to change the output format.

Format

```
/quota/user {-fs <value> | -fsName <value>} [-path <value>] [-userId <value> | -unixName <value> | -winName <value>] [-exceeded] show
```

Object qualifiers

Qualifier	Description
`-fs`	Specify the ID of the file system.
`-fsName`	Specify the name of the file system.
`-path`	Specify either of the following: • If the user quota is for a file system, either do not use this qualifier, or set its value to `/`. • If the user quota is for a quota tree, specify the quota tree path relative to the root of the file system.
`-userId`	Specify the user ID on the file system or quota tree.
`-unixName`	Specify the Unix user name.
`-winName`	Specify the Windows user name. The format is: `[<domain>\]<name>`
`-exceeded`	Only show user quotas whose state is not `OK`.

Example

The following command displays space usage information for user nasadmin on file system res_1, quota tree /qtree_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /quota/user -fs res_1 -path /qtree_1 unixName nasadmin show -detail

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

1:    User ID             = 201
      Unix name           = nasadmin
      Windows names       = dell\nasadmin, dell\nasad
      Windows SIDs        = S-1-5-32-544, S-1-5-32-545
      Space used          = 32768 (32K)
      Soft limit          = 16384 (16K)
      Hard limit          = 65536 (64K)
      Grace period left   = 7d 3h
      State               = Soft limit exceeded
```

Change quota limits for a specific user

You can change limits for user quotas on a file system or quota tree.

Format

/quota/user {-fs | -fsName *<value>*} [-path *<value>*] {-userId *<value>* | -unixName *<value>* | winName *<value>*} set [-async] {-default | [-softLimit *<value>*] [-hardLimit *<value>*]}

Object qualifiers

Qualifier	Description
-fs	Specify the ID of the file system.
-fsName	Specify the name of the file system.
-path	Specify either of the following: • If the user quota is for a file system, either do not use this qualifier, or set its value to /. • If the user quota is for a quota tree, specify the quota tree path relative to the root of the file system.
-userId	Specify the user ID on the file system or quota tree.
-unixName	Specify the UNIX user name associated with the specified user ID.
-winName	Specify the Windows user name associated with the specified user ID. The format is: [<domain>\]<name>

Action qualifiers

Qualifier	Description
-async	Run the operation in asynchronous mode.
-default	Inherit the default quota limit settings for the user. To view the default limit, use the command: config -fs *<value>* -path *<value>* show

Qualifier	Description
	If a soft or hard limit has not been specified for the user, the default limit is applied.
`-softLimit`	Specify the preferred limit on storage usage by the user. A value of `0` means no limitation. If the hard limit is specified and the soft limit is not specified, there will be no soft limitation.
`-hardLimit`	Specify the absolute limit on storage usage by the user. A value of `0` means no limitation. If the soft limit is specified and the hard limit is not specified, there will be no hard limitation. **Note** The hard limit should be larger than the soft limit.

Example

The following command makes the following changes to the user quota for user 201 on file system res_1, quota tree path /qtree_1:

- Sets the soft limit to 10 GB.
- Sets the hard limit to 20 GB.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /quota/user -fs
res_1 -path /qtree_1 -userId 201 set -softLimit 10G -hardLimit 20G
```

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

Operation completed successfully.
```

Refresh user quotas

Because there can be a large amount of user quotas on a file system or quota tree, to reduce the impact on system performance, the system only updates user quota data every 24 hours. Use the refresh action to update the data more often. Use the `/quota/config show` command to view the time spent for the data refresh.

Format

```
/quota/user {-fs <value> | -fsName <value>} [-path <value>]
refresh [-updateNames] [-async]
```

Object qualifiers

Qualifier	Description
`-fs`	Specify the ID of the file system.
`-fsName`	Specify the name of the file system.
`-path`	Specify either of the following: • If the user quota is on a file system, either do not use this qualifier, or set its value to `/`. • If the user quota is on a quota tree, specify the quota tree path relative to the root of the file system.

Qualifier	Description
-updateNames	Refresh the usage data of user quotas and the Windows user names, Windows SIDs, and Unix user names within a file system or quota tree. **Note** Refreshing user names causes latency because the system needs to query the name servers, so use this qualifier sparingly. The system automatically updates Windows user names, Windows SIDs, and Unix user names for user quotas every 24 hours.

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.

Example

The following command refreshes all user quotas on file system res_1, quota tree tree_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /quota/user -fs res_1 -path /tree_1 refresh

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

Operation completed successfully.
```

Manage quota trees

A quota tree is a directory that has a quota applied to it, which limits or tracks the total storage space consumed that directory. The hard limit, soft limit, and grace period settings you define for a quota tree are used as defaults for the quota tree's user quotas. You can override the hard and soft limit settings by explicitly specifying these settings when you create or modify a user quota.

The following table lists the attributes for quota trees:

Table 106 Attributes for quota trees

Attribute	Description
File system	Identifier for the file system.
Path	Quota tree path relative to the root of the file system.
Description	Quota tree description.

Table 106 Attributes for quota trees (continued)

Attribute	Description
`Soft limit`	Preferred limit on storage usage. The system issues a warning when the soft limit is reached.
`Hard limit`	Absolute limit on storage usage. If the hard limit is reached for a quota tree, users will not be able to write data to tree until more space becomes available.
`Grace period left`	Period that counts down time once the soft limit is met. If the quota tree's grace period expires, users cannot write to the quota tree until more space becomes available, even if the hard limit has not been reached.
`State`	State of the user quota. Valid values are: - `OK` - `Soft limit exceeded` - `Soft limit exceeded and grace period expired` - `Hard limit exceeded`

Create a quota tree

Create a quota tree to track or limit the amount of storage consumed on a directory. You can use quota trees to:

- Set storage limits on a project basis. For example, you can establish quota trees for a project directory that has multiple users sharing and creating files in it.
- Track directory usage by setting the quota tree's hard and soft limits to 0 (zero).

Format

```
/quota/tree create [-async] { -fs <value> | -fsName <value>} -
path <value> [-descr <value>] {-default | [-softLimit <value>]
[-hardLimit <value>]}
```

Action qualifiers

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-fs`	Specify the ID of the file system in which the quota tree will reside. The file system cannot be read-only or a replication destination.
`-fsName`	Specify the name of the file system in which the quota tree will reside. The file system cannot be read-only or a replication destination
`-path`	Specify the quota tree path relative to the root of the file system.
`-descr`	Specify the quota tree description.

Qualifier	Description
-default	Specify to inherit the default quota limit settings for the tree. Use the View quota trees on page 415 command to view these default limits.
-softLimit	Specify the preferred limit for storage space consumed on the quota tree. A value of *0* means no limitation. If the hard limit is specified and soft limit is not specified, there will be no soft limitation.
-hardLimit	Specify the absolute limit for storage space consumed on the quota tree. A value of *0* means no limitation. If the soft limit is specified and the hard limit is not specified, there will be no hard limitation. **Note** The hard limit should be larger than the soft limit.

Example

The following command creates quota tree /qtree_1 on file system res_1. The new quota tree has the following characteristics:

- Soft limit is 100 GB.
- Hard limit is 200 GB.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /quota/tree create -fs res_1 -path /qtree_1 -softLimit 100G -hardLimit 200G

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

Operation completed successfully.
```

View quota trees

You can display space usage and limit information for all quota trees on a file system or a single quota tree.

Because there can be a large amount of quota trees on a file system, to reduce the impact on system performance, the system only updates quota data every 24 hours. You can use the refresh action to update the data more often. Use the `/quota/config show` command to view the time spent for the data refresh.

Note

The show action command on page 23 explains how to change the output format.

Format

`/quota/tree {-fs <value> | -fsName <value>} [-path <value>] [-exceeded] show`

Object qualifiers

Qualifier	Description
-fs	Specify the ID of the file system.
-fsName	Specify the name of the file system.

Qualifier	Description
`-path`	Specify the quota tree path, which is relative to the root of the file system.
`-exceeded`	Only show quota trees whose state is not *OK*.

Example

The following command displays space usage information for all quota trees on file system res_1:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /quota/tree -fs res_1 show -detail`

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

1:     Path                  = /qtree_1
       Description           = this is tree 1
       Space used            = 32768 (32K)
       Soft limit            = 53687091200 (50G)
       Hard limit            = 107374182400 (100G)
       Grace period left     = 7d
       State                 = OK

2:     Path                  = /qtree_2
       Description           =
       Space used            = 32768 (32K)
       Soft limit            = 16384 (16K)
       Hard limit            = 65536 (64K)
       Grace period left     = 7d
       State                 = Soft limit exceeded
```

Set quota limits for a specific quota tree

You can specify that a specific quota tree inherit the associated file system's default quota limit settings, or you can manually set soft and hard limits on the quota tree.

Format

`/quota/tree {-fs <value> | -fsName <value>} -path <value> set [-async] [-descr <value>] {-default | [-softLimit <value>] [-hardLimit <value>]}`

Object qualifiers

Qualifier	Description
`-fs`	Specify the ID of the file system.
`-fsName`	Specify the name of the file system.
`-path`	Specify the quota tree path, which is relative to the root of the file system.

Action qualifiers

Qualifier	Description
`-async`	Run the operation in asynchronous mode.

Qualifier	Description
-descr	Quota tree description.
-default	Inherit the default quota limit settings from the associated file system. To view the default limits, use the following command: `/quota/config -fs <value> -path <value> show`
-softLimit	Specify the preferred limit for storage space consumed on the quota tree. A value of 0 means no limitation.
-hardLimit	Specify the absolute limit for storage space consumed on the quota tree. A value of 0 means no limitation. **Note** The hard limit should be equal to or larger than the soft limit.

Example

The following command makes the following changes to quota tree /qtree_1 in file system res_1:

- Sets the soft limit is 50 GB.
- Sets the hard limit is to 100 GB.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /quota/tree -fs
res_1 -path /qtree_1 set -softLimit 50G -hardLimit 100G
```

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

Operation completed successfully.
```

Refresh all quota trees on a file system

Because there can be a large amount of quota trees on a file system, to reduce the impact on system performance, the system only updates quota data every 24 hours. You can use the refresh action to update the data more often. To view the updating time of the data refresh, see the output field Tree quota update time for the `/quota/config show` command.

Format

```
/quota/tree {-fs <value> | -fsName <value>} refresh [-async]
```

Object qualifier

Qualifier	Description
-fs	Specify the ID of the file system.
-fsname	Specify the name of the file system.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.

Example

The following command refreshes quota information for all quota trees on file system res_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /quota/tree -fs
res_1 refresh /
```

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

Operation completed successfully.
```

Delete quota trees

You can delete all quota trees on a file system or a specified quota tree.

Format

```
/quota/tree {-fs <value> | -fsName <value>} -path <value>
delete [-async]
```

Object qualifier

Qualifier	Description
`-fs`	Specify the ID of the file system.
`-fsName`	Specify the name of the file system.
`-path`	Specify either of the following: • To delete all quota trees on the file system, either do not use this qualifier, or set its value to `/`. • To delete a specific quota tree, specify the quota tree path relative to the root of the file system.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.

Example

The following command deletes quota tree `/qtree_1` on file system res_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /quota/tree -fs
res_1 -path /qtree_1 delete
```

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

```
HTTPS connection

Operation completed successfully.
```

Manage quota settings

Managing quota settings includes selecting a quota policy for a file system, setting default limits for a file system or quota tree, setting a default grace period, and disabling the enforcement of space usage limits for a quota tree and user quotas on the tree.

The following table lists the attributes for configuration quota functionality:

Table 107 Attributes for configuring quota functionality

Attribute	Description
`Path`	Quota tree path relative to the root of the file system. For a file system, either do not use this attribute, or set its value to `/`.
`Quota policy`	(Applies to file systems only.) Quota policy for the file system. Valid values are: • `blocks`. Calculates space usage in terms of file system blocks (8 KB units). Block usage depends solely on the number of bytes added to or removed from the file. Any operation resulting in allocating or removing blocks, such as creating, expanding, or deleting a directory, writing or deleting files, or creating or deleting symbolic links changes block usage. When using the blocks policy, a user can create a sparse file whose size is larger than the file size, but that uses fewer blocks on the drive. Optionally, use this policy for NFS-only and multiprotocol file systems. • `filesize` (default). Calculates space usage in terms of logical file sizes and ignores the size of directories and symbolic links. Use the File policy in the following circumstances: ▪ When you have an SMB-only file system ▪ When file sizes are critical to quotas, such as when user usage is based on the size of the files created, and exceeding the size limit is unacceptable.
`User quota`	(Applies to file systems only.) Indicates whether to enforce user quotas on the file system. Valid values are: • on. Enable the enforcement of user quotas on the file system or quota tree. • off. Disable the enforcement of user quotas on the file system or quota tree.

Table 107 Attributes for configuring quota functionality (continued)

Attribute	Description
	Note Because these operations impact system performance, it is recommended that you perform them only during non-peak production hours. When user quota enforcement is enabled, you can change quota settings without impacting performance.
`Deny access`	Indicates whether to enforce quota space usage limits for the file system. Value is one of the following: • yes. (Default) Enforce quota space usage limits for the file system or quota tree. When you choose this option, the ability to allocate space is determined by the quota settings. • no. Do not enforce quota functionality for the file system or quota tree. When you choose this option, the ability to allocate space will not be denied when a quota limit is crossed.
`Grace period`	Time period for which the system counts down days once the soft limit is met. If the grace period expires for a file system or quota tree, users cannot write to the file system or quota tree until more space becomes available, even if the hard limit has not been crossed.
`Default soft limit`	Default preferred limit on storage usage for user quotas on the file system, quota trees in the file system, and user quotas on the quota trees in the file system. The system issues a warning when the soft limit is reached.
`Default hard limit`	Default hard limit for on storage usage for user quotas on the file system, quota trees in the file system, and user quotas on the quota trees in the file system. If the hard limit is reached for a file system or quota tree, users will not be able to write data to the file system or tree until more space becomes available. If the hard limit is reached for a user quota on a file system or quota tree, that user will not be able to write data to the file system or tree.
`Tree quota update time`	Tree quota report updating time. The format is YYYY-MM-DD HH:MM:SS.
`User quota update time`	User quota report updating time. The format is YYYY-MM-DD HH:MM:SS.

Configure quota settings

You can configure quota configuration settings for a file system or quota tree.

Format

```
/quota/config {-fs <value> | -fsName <value>} [-path <value>]
set [-async] {-policy {blocks | filesize} | [-userQuota {on |
off | clear}] [-gracePeriod <value>] [-defaultSoft <value>] [-
defaultHard <value>] [-denyAccess {yes | no}]}
```

Object qualifiers

Qualifier	Description
`-fs`	Specify the ID of the file system for which you are configuring quota settings. The file system cannot be read-only or a replication destination.
`-fsname`	Specify the name of the file system for which you are configuring quota settings. The file system cannot be read-only or a replication destination.
`-path`	Specify the quota tree path relative to the root of the file system. For a file system, either do not use this attribute, or set its value to `/`.

Action qualifiers

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-userQuota`	Indicates whether to enforce user quotas on the file system or quota tree. Valid values are: • `on` - Enable the enforcement of user quotas on the file system or quota tree. • `off` - Disable the enforcement of user quotas on the file system or quota tree. When you disable user quotas, the current user quota settings still exist unless you clear them. These settings are automatically reapplied when user quotas are re-enabled. • `clear` - Clear user quota settings after disabling a user quota. Because enabling and disabling the enforcement of user quotas impacts system performance, it is recommended that you perform these operations only during non-peak production hours. When user quota enforcement is enabled, you can change user quota settings without impacting performance.
`-policy`	Specify the quota policy for the file system. Valid values are: • `blocks` (Blocks policy) - Calculates space usage in terms of file system blocks (8 KB units), and includes drive usage by directories and symbolic links in the calculations. • `filesize` (File policy) - Calculates space usage in terms of logical file sizes, and ignores the size of directories and symbolic links. For more information, see Configure quota settings on page 420
`-gracePeriod`	Specify the time period for which the system counts down days once the soft limit is met. If the grace period expires for a quota tree, users cannot write to the quota tree until more space becomes available, even if the hard limit has not been crossed. If the grace period expires for a user quota on a file system or quota tree, the individual user cannot write to the file system or quota tree until more space becomes available for that user. The default grace period is 7 days. The format is: `<value><qualifier>`

Qualifier	Description
	where: • value - An integer value, depending on the associated qualifier: ▪ If the qualifier is m (minutes), the valid range is from 1 to 525600. ▪ If the qualifier is h (hours), the valid range is from 1 to 8760. ▪ If the qualifier is d (days), the valid range is from 1 to 365. • qualifier - One of the following value qualifiers (case insensitive): ▪ `m` - Minutes ▪ `h` - Hours ▪ `d` - Days
`-defaultSoft`	Specifies the default preferred limit on storage usage for user quotas on the file system, quota trees in the file system, and user quotas on the quota trees in the file system. The system issues a warning when the soft limit is reached.
`-defaultHard`	Specify the default hard limit for on storage usage for user quotas on the file system, quota trees in the file system, and user quotas on the file system's quota trees. If the hard limit is reached for a quota tree, users will not be able to write data to the file system or tree until more space becomes available. If the hard limit is reached for a user quota on a file system or quota tree, that particular user will not be able to write data to the file system or tree. **Note** The hard limit should be larger than the soft limit.
`-denyAccess`	Indicates whether to enable quota limits for the file system. Valid values are: • `yes` - Enable quota functionality for the file system. When you choose this option, the ability to allocate space is determined by the quota settings. • `no` - Disable quota functionality for the file system. When you choose this option, the ability to allocate space will not be denied when a quota limit is reached.

Example

The following command configures quota tree /qtree_1 in file system res_1 as follows:

- Sets the default grace period to 5 days.
- Sets the default soft limit 10 GB.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /quota/config -fs
res_1 -path /qtree_1 set -gracePeriod 5d -defaultSoft 10G
```

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

```
HTTPS connection

Operation completed successfully.
```

View quota configuration settings

You can display the quota configuration settings for a file system, a specific quota tree, or a file system and all of its quota trees.

Format

/quota/config {-fs *<value>* | -fsName *<value>*} [-path *<value>*] show

Object qualifiers

Qualifier	Description
-fs	Specify the ID of the file system.
-fsname	Specify the name of the file system.
-path	Specify the quota tree path relative to the root of the file system. For a file system, either do not use this attribute, or set its value to /. If this value is not specified, the command displays the quota configuration of the file system level and the quota configuration of all quota tree within the specified file system.

Example

The following command lists configuration information for quota tree /quota/config on file system res_1:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /quota/config -fs res_1 show -detail

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

1:    Path                      = /
      Quota policy              = blocks
      User quota                = on
      Deny access               = yes
      Grace period              = 7d
      User soft limit           = 53687091200 (50G)
      User hard limit           = 107374182400 (100G)
      Tree quota update time    = 2014-10-31 13:17:28
      User quota update time    = 2014-10-31 13:20:22

2:    Path                      = /qtree_1
      Quota policy              = blocks
      User quota                = on
      Deny access               = yes
      Grace period              = 7d
      User soft limit           = 1073741824 (1G)
      User hard limit           = 10737418240 (10G)
      Tree quota update time    =
      User quota update time    =
```

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 108 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 path relative to the file system of the directory that the share will provide access to. Default is /root of the file system. A local path must point to an existing directory within the file system.
`Export path`	Export path, used by hosts to connect to the share. **Note** The export path is a combination of the network name or IP address 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` — Hosts have read-only access to primary storage and snapshots associated with the share. • `rw` — Hosts have read/write access to primary storage and snapshots associated with the share. • `roroot` — Hosts have read-only access to primary storage and snapshots associated with the share, but the root of the NFS client has root access. • `root` — Hosts have read/write root access to primary storage and snapshots associated with the share. This includes the ability to set access controls that

Table 108 NFS network share attributes (continued)

Attribute	Description
	restrict the permissions for other login accounts. - `na` — Hosts have no access to the share or its snapshots.
`Advanced host management enabled`	Indicates whether host lists are configured by specifying the IDs of registered hosts or by using a string. (A registered host is defined by using the `/remote/host command`.) Values are (case insensitive): - `yes` (default) — Hosts lists contain the IDs of registered hosts. - `no` — Host lists contain comma-separated strings, with each string defining a hostsname, IP, subnet, netgroup, or DNS domain. For information about specifying host lists by using a string, see Specifying host lists by using a string on page 427.
`Read-only hosts`	Comma-separated list of hosts that have read-only access to the share and its snapshots. If advanced host management is enabled, this is a list of the IDs of registered hosts. Otherwise, this is a list of network host names, IPs, subnets, domains, or netgroups.
`Read/write hosts`	Comma-separated list of hosts that have read-write access to the share and its snapshots. If advanced host management is enabled, this is a list of the IDs of registered hosts. Otherwise, this is a list of network host names, IPs, subnets, domains, or netgroups.
`Read-only root hosts`	Comma-separated list of hosts that have read-only root access to the share and its snapshots. If advanced host management is enabled, this is a list of the IDs of registered hosts. Otherwise, this is a list of network host names, IPs, subnets, domains, or netgroups.
`Root hosts`	Comma-separated list of hosts that have read-write root access to the share and its snapshots. If advanced host management is enabled, this is a list of the IDs of registered hosts. Otherwise, this is a list of network host names, IPs, subnets, domains, or netgroups.
`No access hosts`	Comma-separated list of hosts that have no access to the share or its snapshots. If advanced host management is enabled, this is

Table 108 NFS network share attributes (continued)

Attribute	Description
	a list of the IDs of registered hosts. Otherwise, this is a list of network host names, IPs, subnets, domains, or netgroups.
`Allow SUID`	Specifies whether to allow users to set the `setuid` and `setgid` Unix permission bits. Values are (case insensitive): • `yes` (default) — Users can set the `setuid` and `setgid` Unix permission bits. This allows users to run the executable with privileges of the file owner. • `no` — Users cannot set the `setuid` and `setgid` Unix permission bits.
`Anonymous UID`	(Applies when the host does not have `"allow root"` access provided to it.) UID of the anonymous account. This account is mapped to client requests that arrive with a user ID of 0 (zero), which is typically associated with the user name `root`. The default value is 4294967294 (-2), which is typically associated with the `nobody` user (root squash).
`Anonymous GID`	(Applies when the host does not have `"allow root"` access provided to it.) GID of the anonymous account. This account is mapped to client requests that arrive with a user ID of 0 (zero), which is typically associated with the user name `root`. The default value is 4294967294 (-2), which is typically associated with the `nobody` user (root squash).
`Creation time`	Creation time of the share.
`Last modified time`	Last modified time of the share.
`Role`	The specific usage of the file share. Value is one of the following: • `production` — default for source NAS server. • `backup` — default for destination NAS server. Automatically set for all shares created on a NAS server that is acting as a replication destination. In other cases `production` is automatically set as a role for the NFS Share

Table 108 NFS network share attributes (continued)

Attribute	Description
`Minimum security`	Specifies a minimal security option that must be provided by client for nfs mount operation (in fstab). Value is one of the following, from lower to higher security level: • `sys` — No server-side authentication (server relies on NFS client authentication). Without a configured secure NFS for the NAS server this setting is default (aka AUTH_SYS security). • `krb5` — Kerberos v5 authentication. Default when secure NFS is configured for the NAS server. • `krb5i` — Kerberos v5 authentication and integrity. • `krb5p` — Kerberos v5 authentication and integrity; encryption is enabled.

Specifying host lists by using a string
If advanced host management is disabled, a host list can contain a combination of network host names, IP addresses, subnets, netgroups, or DNS domains. The following formatting rules apply:

- An IP address can be an IPv4 or IPv6 address.
- A subnet can be an IP address/netmask or IP address/prefix length (for example: `168.159.50.0/255.255.255.0` or `168.159.50.0/24`).
- The format of the DNS domain follows the UNIX/Linux format; for example, *.example.com. When specifying wildcards in fully qualified domain names, dots are not included in the wildcard. For example, `*.example.com` includes `one.example.com`, but does not include `one.two.example.com`.
- To specify that a name is a netgroup name, prepend the name with @. Otherwise, it is considered to be a host name.

If advanced host management is enabled, host lists contain the host IDs of existing hosts. You can obtain these IDs by using the `/remote/host` command.

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. Create file systems on page 394 explains how to create file systems on the system.

Format

```
/stor/prov/fs/nfs create [-async] –name <value> [-descr
<value>] {-fs <value> | -fsName <value>} -path <value> [-
defAccess {ro |rw | roroot | root | na}] [-advHostMgmtEnabled
{yes | no}] [-roHosts <value>] [-rwHosts <value>] [-roRootHosts
<value>] [-rootHosts <value>] [-naHosts <value>] [-minSecurity
{sys | krb5 | krb5i | krb5p}] [-allowSuid {yes | no}] [-anonUid
<value>] [-anonGid <value>]
```

Action qualifiers

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-name`	Type a name for the share. By default, this value, along with the network name or the IP address of the NAS server, constitutes the export path by which hosts access the share. You can use the forward slash character (/) to create a " virtual" name space that is different from the real path name used by the share. For example, `/fs1` and `/fs2` can be represented as `vol/fs1` and `vol/fs2`. The following considerations apply: • You cannot use the / character as the first character of the share name. • An NFSv4 client cannot mount a share using a name that contains the / character. Instead the client must use the share path. To use the share path, you must set the NAS server parameter `nfs.showExportLevel` to 0 or 1.
`-descr`	Type a brief description of the share.
`-fs`	Type the ID of the parent file system associated with the NFS share.
`-fsName`	Type the name 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 initial share is created on the root of the file system.

Qualifier	Description
	• Before you can create additional network shares within an NFS file system, you must create directories within the file system. Connect to the initial NFS share from a host with access to the share and set access permissions accordingly.
`-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` — Hosts have read-only access to primary storage and snapshots associated with the share. • `rw` — Hosts have read/write access to primary storage and snapshots associated with the share. • `roroot` — Hosts have read-only access to primary storage and snapshots associated with the share. The root of the NFS client has root access. • `root` — Hosts have 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` (default) — Hosts have no access to the share or its snapshots.
`-advHostMgmtEnabled`	Specify whether host lists are configured by specifying the IDs of registered hosts or by using a string. (A registered host is defined by using the `/remote/host command`.) Values are (case insensitive): • `yes` (default) — Hosts lists contain the IDs of registered hosts. • `no` — Host lists contain comma-separated strings, with each string defining a hostsname, IP, subnet, netgroup, or DNS domain. For information about specifying host lists by using a string, see Specifying host lists by using a string on page 427.
`-roHosts`	Type the IDs of hosts that have read-only access to the share and its snapshots. Separate the IDs with commas. If advanced host management is enabled, this is a list of the IDs of registered hosts. Otherwise, this is a list of network host names, IPs, subnets, domains, or netgroups.
`-rwHosts`	Type the IDs of hosts that have read-write access to the share and its snapshots. Separate the IDs with commas. If advanced host management is enabled, this is a list of the IDs of registered hosts. Otherwise, this is a list of network host names, IPs, subnets, domains, or netgroups.

Qualifier	Description
`-roRootHosts`	Type the IDs of hosts that have read-only root access to the share and its snapshots. Separate the IDs with commas. If advanced host management is enabled, this is a list of the IDs of registered hosts. Otherwise, this is a list of network host names, IPs, subnets, domains, or netgroups.
`-rootHosts`	Type the IDs of hosts that have read-write root access to the share and its snapshots. Separate the IDs with commas. If advanced host management is enabled, this is a list of the IDs of registered hosts. Otherwise, this is a list of network host names, IPs, subnets, domains, or netgroups.
`-naHosts`	Type the ID of each host configuration for which you want to block access to the share and its snapshots. Separate the IDs with commas. If advanced host management is enabled, this is a list of the IDs of registered hosts. Otherwise, this is a list of network host names, IPs, subnets, domains, or netgroups.
`-minSecurity`	Specify a minimal security option that must be provided by client for nfs mount operation (in fstab). Value is one of the following, from lower to higher security level. All higher security levels are supported, and can be enforced by the client at negotiations for secure NFS access. • `sys` — No server-side authentication (server relies on NFS client authentication). Without a configured secure NFS for the NAS server this setting is default. • `krb5` — Kerberos v5 authentication. Default when secure NFS is configured for the NAS server. • `krb5i` — Kerberos v5 authentication and integrity. • `krb5p` — Kerberos v5 authentication and integrity; encryption is enabled.
`-allowSuid`	Specifies whether to allow users to set the `setuid` and `setgid` Unix permission bits. Values are (case insensitive): • `yes` (default) — Users can set the `setuid` and `setgid` Unix permission bits. This allows users to run the executable with privileges of the file owner. • `no` — Users cannot set the `setuid` and `setgid` Unix permission bits.
`-anonUid`	Specify the UID of the anonymous account.
`-anonGid`	Specify the GID of the anonymous account.

Example 1

The following command shows output for when the path is not found because the path does not start with "/", and the shares are not created successfully.

```
uemcli -u admin -p Password123! /stor/prov/fs/nfs create -name
testnfs112 -fs res_26 -path "mypath"
```

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

Operation failed. Error code: 0x900a002
The system could not find the specified path. Please use an
existing path. (Error Code:0x900a002)
Job ID = N-1339
```

Example 2

The following command shows output for when the path is correctly specified and the shares are successfully created. The new NFS share has the following settings:

- NFS share name of "testnfs112"
- Parent file system of "res_26"
- On the directory "/mypath"

```
uemcli -u admin -p Password123! /stor/prov/fs/nfs create -name
testnfs112 -fs res_26 -path "/mypath"
```

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

ID = NFSShare_20
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 23 explains how to change the output format.

Format

/stor/prov/fs/nfs [{-id *<value>* | -name *<value>* | -fs *<value>* | -fsName *<value>*}] show

Object qualifiers

Qualifier	Description
-id	Type the ID of an NFS share.
-name	Type the name of an NFS share.
-fs	Type the ID of an NFS file system to view the associated NFS network shares.
-fsName	Type the name 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                       = NFSShare_1
        Name                     = MyNFSshare1
        Description              = My nfs share
        File system              = res_26
        Local path               = /mypath
        Export path              = SATURN.domain.emc.com:/MyNFSshare1
        Default access           = na
        Advanced host mgmt.      = yes
        Read-only hosts          = 1014, 1015
        Read/write hosts         = 1016
        Read-only root hosts     =
        Root hosts               =
        No access hosts          =
        Creation time            = 2012-08-24 12:18:22
        Last modified time       = 2012-08-24 12:18:22
        Role                     = production
        Minimum security         = krb5
        Allow SUID               = yes
        Anonymous UID            = 4294967294
        Anonymous GID            = 4294967294
```

Change NFS share settings

Change the settings of an NFS share.

Format

```
/stor/prov/fs/nfs {-id <value> | -name <value>} set [-async][-
descr <value>] [-defAccess {ro | rw | roroot | root | na}] [-
advHostMgmtEnabled {yes | no}] [-roHosts <value>] [-rwHosts
<value>] [-roRootHosts <value>] [-rootHosts <value>] [-naHosts
<value>] [-minSecurity {sys | krb5 | krb5i | krb5p}] [-
allowSuid { yes | no }] [-anonUid <value>] [-anonGid <value>]
```

Object qualifiers

Qualifier	Description
`-id`	Type the ID of an NFS share to change. View NFS share settings on page 431 explains how to view the IDs of the NFS network shares on the system.
`-name`	Type the name of an NFS share to change.

Action qualifiers

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:

Qualifier	Description
	• `ro` – Hosts have read-only access to primary storage and snapshots associated with the share. • `rw` – Hosts have read/write access to primary storage and snapshots associated with the share. • `roroot` – Hosts have read-only root access to primary storage and snapshots associated with the share. • `root` – Hosts have 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` – Hosts have no access to the share or its snapshots.
`-advHostMgmtEnabled`	Specify whether host lists are configured by specifying the IDs of registered hosts or by using a string. (A registered host is defined by using the `/remote/host command`.) Values are (case insensitive): • `yes` (default) — Hosts lists contain the IDs of registered hosts. • `no` — Host lists contain comma-separated strings, with each string defining a hostsname, IP, subnet, netgroup, or DNS domain
`-roHosts`	Type the IDs of hosts that have read-only access to the share and its snapshots. Separate the IDs with commas. If advanced host management is enabled, this is a list of the IDs of registered hosts. Otherwise, this is a list of network host names, IPs, subnets, domains, or netgroups.
`-rwHosts`	Type the IDs of hosts that have read-write access to the share and its snapshots. Separate the IDs with commas. If advanced host management is enabled, this is a list of the IDs of registered hosts. Otherwise, this is a list of network host names, IPs, subnets, domains, or netgroups.
`-roRootHosts`	Type the IDs of hosts that have read-only root access to the share and its snapshots. Separate the IDs with commas. If advanced host management is enabled, this is a list of the IDs of registered hosts. Otherwise, this is a list of network host names, IPs, subnets, domains, or netgroups.
`-rootHosts`	Type the IDs of hosts that have read-write root access to the share and its snapshots. Separate the IDs with commas. If advanced host management is enabled, this is a list of the IDs of registered hosts. Otherwise, this is a list of network host names, IPs, subnets, domains, or netgroups.

Qualifier	Description
`-naHosts`	Type the ID of each host configuration for which you want to block access to the share and its snapshots. Separate the IDs with commas. If advanced host management is enabled, this is a list of the IDs of registered hosts. Otherwise, this is a list of network host names, IPs, subnets, domains, or netgroups
`-minSecurity`	Specifies a minimal security option that must be provided by client for NFS mount operation. Value is one of the following, from lower to higher security level. All higher security levels are supported, and can be enforced by the client at negotiations for secure NFS access. • `sys` - No server-side authentication (server relies on NFS client authentication). Also known as `AUTH_SYS` security. • `krb5` - Kerberos v5 authentication. • `krb5i` - Kerberos v5 authentication and integrity. • `krb5p` - Kerberos v5 authentication and integrity; encryption is enabled.
`-allowSuid`	Specifies whether to allow users to set the `setuid` and `setgid` Unix permission bits. Values are (case insensitive): • `yes` (default) Users can set the `setuid` and `setgid` Unix permission bits. This allows users to run the executable with privileges of the file owner. • `no` - Users cannot set the `setuid` and `setgid` Unix permission bits.
`-anonUid`	Specify the UID of the anonymous account.
`-anonGid`	Specify the GID of the anonymous account.

Example

The following command changes NFS share NFSShare_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 NFSShare_1 set -descr “My share” -naHosts ”HOST_1”
```

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

ID = NFSShare_1
Operation completed successfully.
```

Delete NFS network shares

Delete an NFS share.

Format

```
/stor/prov/fs/nfs {-id <value> | -name <value>} delete [-async]
```

Object qualifiers

Qualifier	Description
`-id`	Type the ID of an NFS share to change. View NFS share settings on page 431 explains how to view the IDs of the NFS network shares on the system.
`-name`	Type the name of an NFS share to change.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.

Example

The following command deletes NFS share NFSShare_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs/nfs –
id NFSShare_1 delete
```

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

Operation completed successfully.
```

Manage SMB network shares

Server Message Block (SMB) network shares use the SMB (formerly known as CIFS) protocol to provide an access point for configured Windows hosts, or IP subnets, to access file system storage. SMB network shares are associated with a SMB file system.

Each SMB share is identified by an ID.

The following table lists the attributes for SMB network shares:

Table 109 SMB 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 within the file system that the share provides access to.
`Export path`	Export path, used by hosts to connect to the share.

Table 109 SMB network share attributes (continued)

Attribute	Description
	Note The export path is a combination of the network name or the IP address of the associated NAS server and the name of the share.
`File system`	ID of the parent file system associated with the SMB share.
`Creation time`	Creation time of the share.
`Last modified time`	Last modified time of the share.
`Availability enabled`	Continuous availability state.
`Encryption enabled`	SMB 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)
`Offline availability`	Indicates whether Offline availability is enabled. When enabled, users can use this feature on their computers to work with

Table 109 SMB network share attributes (continued)

Attribute	Description
	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 (SMB) 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 394 explains how to create file systems on the system.

Format

```
/stor/prov/fs/cifs create [-async] –name <value> [-descr
<value>] {-fs <value> | -fsName <value>} -path <value> [-
enableContinuousAvailability {yes|no}] [-enableCIFSEncryption
{yes|no}] [-umask <value> ] [-enableABE {yes | no} ] [-
enableBranchCache {yes | no}] [-offlineAvailability {none |
documents | programs | manual} ]
```

Action qualifiers

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.

Qualifier	Description
`-fsName`	Type the name of the parent file system associated with the CIFS share.
`-path`	Type the path to the directory within the file system that will be shared. This path must correspond to an existing directory/ folder name within the share that was created from the host-side. The default path is the root of the file system. Local paths must point to an existing directory within the file system. • The same path on a file system can be shared an unlimited number of times, but each share name must be unique. The initial share will be created on the file system root directory. • Before you can create additional network shares or subdirectories within an NFS file system, you must create network shares or subdirectories 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` (default)
`-enableBranchCache`	Specify if BranchCache is enabled. Valid values include: • `yes` • `no` (default)
`-offlineAvailability`	Specify the type of offline availability. Valid values include: • `none` (default) — Prevents clients from storing documents and programs in offline cache.

Qualifier	Description
	• 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 res_1.
- Local path on the file system is directory "/cifsshare".
- Continuous availability is enabled.
- CIFS encryption is enabled.

The share receives ID CIFSShare_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 (SMB) 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 23 explains how to change the output format.

Format

```
/stor/prov/fs/cifs [{-id <value> | -name <value> | -fs <value>
| -fsName <value>}]show
```

Object qualifiers

Qualifier	Description
-id	Type the ID of a CIFS share.
-name	Type the name of a CIFS share.

Qualifier	Description
`-fs`	Type the ID of a CIFS file system to view the associated CIFS network shares.
`-fsName`	Type the name of a CIFS file system to view the associated CIFS network shares.

Example

The following command lists details for all CIFS 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            = SMBShare_1
        Name          = fsmup
        Description   =
        File system   = res_1
        Local path    = /
        Export path   = \\sys-123.abc.xyz123.test.lab.emc.com\fsmup, \
\10.0.0.0\fsmup

2:      ID            = SMBShare_2
        Name          = fsmup
        Description   =
        File system   = res_5
        Local path    = /
        Export path   = \\sys-123.abc.xyz123.test.lab.emc.com\fsmup, \
\10.0.0.0\fsmup
```

Change CIFS share settings

Change the settings of an CIFS (SMB) share.

Format

`/stor/prov/fs/cifs {-id` *`<value>`* `| -name` *`<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 qualifiers

Qualifier	Description
`-id`	Type the ID of a CIFS share to change.
`-name`	Type the name of a CIFS share to change.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.

Qualifier	Description
-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 — Prevents clients from storing documents and programs in offline cache. • documents — Allows all files that users open to be available offline. • 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 SMBShare_1 to `My share`.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs/cifs –id SMBShare_1 set -descr “My share”
```

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

ID = SMBShare_1
Operation completed successfully.
```

Delete CIFS network shares

Delete a CIFS (SMB) share.

Format

```
/stor/prov/fs/cifs {-id <value> | -name <value>} delete [-async]
```

Object qualifiers

Qualifier	Description
`-id`	Type the ID of a CIFS share to delete.
`-name`	Type the name of a CIFS share to delete.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.

Example

The following command deletes CIFS share CIFSShare_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs/cifs –id CIFSShare_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 identifier (LUN ID).

The following table lists the attributes for LUNs:

Table 110 LUN attributes

Attribute	Description
`ID`	ID of the LUN.
`Name`	Name of the LUN.
`Description`	Brief description of the LUN.
`Group`	Name of the consistency group of which the LUN is a member.
`Storage pool ID`	ID of the storage pool the LUN is using.
`Storage pool`	Name of the storage pool the LUN is using.

Table 110 LUN attributes (continued)

Attribute	Description
`Type`	Type of LUN. Value is one of the following (case insensitive): • `Primary` • `Thin clone` (**tc** when used with the `-create` command.)
`Base storage resource`	(Applies to thin clones only) ID of the base LUN for the thin clone.
`Source`	(Applies to thin clones only) ID of the source snapshot for the thin clone.
`Original parent`	(Applies to thin clones only) ID of the parent LUN for the thin clone.
`Health state`	Health state of the LUN. The health state code appears in parentheses. Value is one of the following: • `OK (5)`—The LUN 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. ▪ Resource is unavailable.
`Health details`	Additional health information.
`Size`	Current size of the LUN.

Table 110 LUN attributes (continued)

Attribute	Description
`Maximum size`	Maximum size of the LUN.
`Thin provisioning enabled`	Identifies whether thin provisioning is enabled. Valid values are: • `yes` • `no` (default) 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 subscribed to support more storage capacity than they actually possess. **Note** The Unisphere online help provides more details on thin provisioning.
`Data Reduction enabled`	Identifies whether data reduction is enabled. Valid values are: • `yes` • `no` (default) **Note** Data reduction is available for thin LUNs in an All-Flash pool only.
`Data Reduction space saved`	Total space saved for the LUN (in gigabytes) by using data reduction. **Note** Data reduction is available for thin LUNs in an All-Flash pool only.
`Data Reduction percent`	Total storage percentage saved for the LUN by using data reduction. **Note** Data reduction is available for thin LUNs in an All-Flash pool only.
`Data Reduction ratio`	Ratio between data without data reduction and data after data reduction savings. **Note** Data reduction is available for thin LUNs in an All-Flash pool only.
`Advanced deduplication enabled`	Identifies whether advanced deduplication is enabled for this LUN. This option is available only after data reduction has been enabled. An empty value indicates that advanced deduplication is not supported on the LUN. Valid values are:

Table 110 LUN attributes (continued)

Attribute	Description
	- yes - no (default) **Note** Advanced deduplication is available on Unity All-Flash 450F, 550F, and 650F systems only.
Current allocation	If thin provisioning is enabled, the quantity of primary storage currently allocated through thin provisioning.
Non-base size used	(Applies to standard LUNs only) Quantity of the storage used for the snapshots and thin clones associated with this LUN.
Family size used	(Applies to standard LUNs only) Quantity of the storage used for the whole LUN family.
Snapshot count	Number of snapshots created on the LUN.
Family snapshot count	(Applies to standard LUNs only) Number of snapshots created in the LUN family, including all derivative snapshots.
Family thin clone count	(Applies to standard LUNs only) Number of thin clones created in the LUN family, including all derivative thin clones.
Protection schedule	ID of a protection schedule applied to the LUN. View protection schedules on page 106 explains how to view the IDs of the schedules on the system.
Protection schedule paused	Identifies whether an applied protection schedule is currently paused.
WWN	World Wide Name of the LUN.
Replication destination	Identifies whether the storage resource is a destination for a replication session (local or remote). Valid values are: - yes - no
Creation time	Time the resource was created.
Last modified time	Time the resource was last modified.
SP owner	Identifies the default owner of the LUN. Value is SP A or SP B.
Trespassed	Identifies whether the LUN is trespassed to the peer SP. Valid values are: - yes - no
FAST VP policy	FAST VP tiering policy for the LUN. This policy defines both the initial tier placement and the ongoing automated tiering of data during data relocation operations. Valid values (case-insensitive):

Table 110 LUN attributes (continued)

Attribute	Description
	• `startHighThenAuto` (default)—Sets the initial data placement to the highest-performing drives with available space, and then relocates portions of the storage resource's data based on I/O activity. • `auto`—Sets the initial data placement to an optimum, system-determined setting, and then relocates portions of the storage resource's data based on the storage resource's performance statistics such that data is relocated among tiers according to I/O activity. • `highest`—Sets the initial data placement and subsequent data relocation (if applicable) to the highest-performing drives with available space. • `lowest`—Sets the initial data placement and subsequent data relocation (if applicable) to the most cost-effective drives with available space.
`FAST VP distribution`	Percentage of the LUN assigned to each tier. The format is: `<tier_name>:<value>%` where: • `<tier_name>` is the name of the storage tier. • `<value>` is the percentage of storage in that tier.
`LUN access hosts`	List of hosts with access permissions to the LUN.
`Host LUN IDs`	Comma-separated list of HLUs (Host LUN identifiers), which the corresponding hosts use to access the LUN.
`Snapshots access hosts`	List of hosts with access to snapshots of the LUN.
`IO limit`	Name of the host I/O limit policy applied.
`Effective maximum IOPS`	The effective maximum IO per second for the LUN. For LUNs with a density-based IO limit policy, this value is equal to the product of the `Maximum IOPS` and the `Size` of the attached LUN.
`Effective maximum KBPS`	The effective maximum KBs per second for the LUN. For LUNs with a density-based IO limit policy, this value is equal to the product of the `Maximum KBPS` and the `Size` of the attached 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 drive to the pool. Configure custom pools on page 344 explains how to create a custom storage pool on the system.

Format

```
/stor/prov/luns/lun create [-async] -name <value> [-descr
<value>] [-type {primary | tc {-source <value> | -sourceName
<value>}] [{-group <value> | groupName <value>}] [ {-pool
<value> | -poolName <value>}] [-size <value>] [-thin {yes |
no}] [-sched <value> [-schedPaused {yes | no}]] [-spOwner {spa
| spb}] [-fastvpPolicy {startHighThenAuto | auto | highest |
lowest}] [-lunHosts <value> [-hlus <value>]] [-snapHosts
<value>] [-replDest {yes | no}] [-ioLimit <value>] [-
dataReduction {yes [-advancedDedup {yes | no}] | no}]
```

Action qualifiers

Qualifier	Description
-async	Run the operation in asynchronous mode.
-name	Type the name of the LUN.
-descr	Type a brief description of the LUN.
-type	Specify the type of LUN. Valid values are (case insensitive): • primary (default) • tc
-source	(Applies to thin clones only) Specify the ID of the source object to use for thin clone creation.
-sourceName	(Applies to thin clones only) Specify the name of the source object to use for thin clone creation.
-group	(Not applicable when creating a thin clone) Type the ID of a consistency group to which to associate the new LUN. View consistency groups on page 462 explains how to view information on consistency groups. **Note** If no consistency group is specified with -group or –groupName, the LUN is not assigned to a consistency group.
-groupName	(Not applicable when creating a thin clone) Type the name of a consistency group to which to associate the new LUN. **Note** If no consistency group is specified with -group or –groupName, the LUN is not assigned to a consistency group.
-pool	(Not applicable when creating a thin clone) Type the ID of the storage pool that the LUN will use. **Note** Value is case-insensitive. View pools on page 355 explains how to view the names of the storage pools on the system.

Qualifier	Description
`-poolName`	(Not applicable when creating a thin clone) Type the name of the storage pool that the LUN will use.
`-size`	(Not applicable when creating a thin clone) Type the quantity of storage to allocate for the LUN.
`-thin`	(Not applicable when creating a thin clone) Enable thin provisioning on the LUN. Valid values are: • `yes` • `no` (default)
`-sched`	Type the ID of a protection schedule to apply to the storage resource. View protection schedules on page 106 explains how to view the IDs of the schedules on the system.
`-schedPaused`	Pause the schedule specified for the `-sched` qualifier. Valid values are: • `yes` • `no` (default)
`-spOwner`	(Not applicable when creating a thin clone) Specify the default SP to which the LUN will belong. The storage system determines the default value. Valid values are: • `spa` • `spb`
`-fastvpPolicy`	(Not applicable when creating a thin clone) Specify the FAST VP tiering policy for the LUN. This policy defines both the initial tier placement and the ongoing automated tiering of data during data relocation operations. Valid values (case-insensitive): • `startHighThenAuto` (default)—Sets the initial data placement to the highest-performing drives with available space, and then relocates portions of the storage resource's data based on I/O activity. • `auto`—Sets the initial data placement to an optimum, system-determined setting, and then relocates portions of the storage resource's data based on the storage resource's performance statistics such that data is relocated among tiers according to I/O activity. • `highest`—Sets the initial data placement and subsequent data relocation (if applicable) to the highest-performing drives with available space. • `lowest`—Sets the initial data placement and subsequent data relocation (if applicable) to the most cost-effective drives with available space.
`-lunHosts`	Specify a comma-separated list of hosts with access to the LUN.
`-hlus`	Specifies the comma-separated list of Host LUN identifiers to be used by the corresponding hosts which were specified in the `-lunHosts` option. The number of items in the two lists must

Qualifier	Description
	match. However, an empty string is a valid value for any element of the Host LUN identifiers list, as long as commas separate the list elements. Such an empty element signifies that the system should automatically assign the Host LUN identifier value by which the corresponding host will access the LUN. If not specified, the system will automatically assign the Host LUN identifier value for every host specified in the `-lunHosts` argument list.
`-snapHosts`	Specify a comma-separated list of hosts with access to snapshots of the LUN.
`-replDest`	(Not applicable when creating a thin clone) Specifies whether the resource is a replication destination. Valid values are: • `yes` • `no` (default)
`-ioLimit`	Specify the name of the host I/O limit policy to be applied.
`-dataReduction`	(Not applicable when creating a thin clone) Specify whether data reduction is enabled for this LUN. Valid values are: • `yes` • `no` (default) **Note** Data reduction is available for thin LUNs in an All-Flash pool only.
`-advancedDedup`	Specify whether advanced deduplication is enabled for this LUN. This option is available only after data reduction has been enabled. An empty value indicates that advanced deduplication is not supported on the LUN. Valid values are: • `yes` • `no` (default) **Note** Advanced deduplication is available on Unity All-Flash 450F, 550F, and 650F systems only.

Example 1

The following command creates a LUN with these settings:

- Name is MyLUN.
- Description is “My LUN.”
- Associated with LUN consistency 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" -type primary -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.
```

Example 2

The following command creates a thin clone called MyTC from SNAP_1. The thin clone receives the ID lun_3.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/lun
create -name "MyTC" -descr "My FC" -type tc -source SNAP_1
```

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

ID = lun_3
Operation completed successfully.
```

View LUNs

Display the list of existing LUNs.

Note

The show action command on page 23 explains how to change the output format.

Format

```
/stor/prov/luns/lun [{-id <value> | name <value> | -group
<value> | -groupName <value> | -standalone}] [-type {primary |
tc [{-baseRes <value> | -baseResName <value> | -originalParent
<value> | -originalParentName <value> | -source <value> | -
sourceName <value>}]}] show
```

Object qualifiers

Qualifier	Description
-id	Type the ID of a LUN.
-name	Type the name of a LUN.
-group	Type the ID of a consistency group. The list of LUNs in the specified consistency group are displayed.
-groupName	Type the name of a consistency group. The list of LUNs in the specified consistency group are displayed.
-standalone	Displays only LUNs that are not part of a consistency group.
-type	Identifies the type of resources to display. Valid values are (case insensitive):

Qualifier	Description
	• primary • tc
-baseRes	(Applies to thin clones only) Type the ID of a base LUN by which to filter thin clones.
-baseResName	(Applies to thin clones only) Type the name of a base LUN by which to filter thin clones.
-originalParent	(Applies to thin clones only) Type the ID of a parent LUN by which to filter thin clones.
-originalParentName	Applies to thin clones only) Type the name of a parent LUN by which to filter thin clones.
-source	(Applies to thin clones only) Type the ID of a source snapshot by which to filter thin clones.
-sourceName	(Applies to thin clones only) Type the name of a source snapshot by which to filter thin clones.

Example 1

The following command displays information about all LUNs and thin clones on the system:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/lun show -detail`

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

1:    ID                             = sv_1
      Name                           = AF LUN 1
      Description                    =
      Group                          =
      Storage pool ID                = pool_1
      Storage pool                   = Pool 1
      Type                           = Primary
      Base storage resource          = sv_1
      Source                         =
      Original parent                =
      Health state                   = OK (5)
      Health details                 = "The LUN is operating
normally. No action is required."
      Size                           = 21474836480 (20.0G)
      Maximum size                   = 281474976710656 (256.0T)
      Thin provisioning enabled      = yes
      Compression enabled            = yes
      Compression space saved        = 5637144576 (5.2G)
      Compression percent            = 44%
      Compression ratio              = 1.8:1
      Data Reduction enabled         = yes
      Data Reduction space saved     = 5637144576 (5.2G)
      Data Reduction percent         = 44%
      Data Reduction ratio           = 1.8:1
      Advanced deduplication enabled = no
      Current allocation             = 4606345216 (4.2G)
      Protection size used           = 0
      Non-base size used             = 0
      Family size used               = 12079595520 (11.2G)
      Snapshot count                 = 2
```

```
       Family snapshot count           = 2
       Family thin clone count         = 0
       Protection schedule             = snapSch_1
       Protection schedule paused      = no
       WWN                             =
 60:06:01:60:10:00:43:00:B7:15:A5:5B:B1:7C:01:2B
       Replication destination         = no
       Creation time                   = 2018-09-21 16:00:55
       Last modified time              = 2018-09-21 16:01:41
       SP owner                        = SPB
       Trespassed                      = no
       LUN access hosts                = Host_2
       Host LUN IDs                    = 0
       Snapshots access hosts          =
       IO limit                        =
       Effective maximum IOPS          = N/A
       Effective maximum KBPS          = N/A
```

Change LUNs

Change the settings for a LUN.

Format

```
/stor/prov/luns/lun {-id <value> | -name <value>} set [-async] [-name <value>] [-descr <value>] [-size <value>] [{-group <value> | -groupName <value> | -standalone}] [{-sched <value> | -noSched}] [-schedPaused {yes | no}] [-spOwner {spa | spb}] [-fastvpPolicy {startHighThenAuto | auto | highest | lowest}] [-lunHosts <value> [-hlus <value>]] [-snapHosts <value>] [-replDest {yes | no}] [-ioLimit <value> | -noIoLimit] [-dataReduction {yes [-advancedDedup {yes | no}] | no}]
```

Object qualifiers

Qualifier	Description
`-id`	Type the ID of the LUN to change.
`-name`	Type the name of the LUN to change.

Action qualifiers

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`	(Not applicable to thin clones) Type the ID of a consistency group to which to associate the new LUN. View consistency groups on page 462 explains how to view information on consistency groups. **Note** If no consistency group is specified with `-group` or `–groupName`, the LUN is not assigned to a consistency group.

Qualifier	Description
`-groupName`	(Not applicable to thin clones) Type the name of a consistency group to which to associate the new LUN. **Note** If no consistency group is specified with `-group` or `-groupName`, the LUN is not assigned to a consistency group.
`-size`	Type the quantity of storage to allocate for the LUN.
`-standalone`	(Not applicable to thin clones) Remove the LUN from the consistency group.
`-sched`	Type the ID of the schedule to apply to the LUN. View protection schedules on page 106 explains how to view the IDs of the schedules on the system.
`-schedPaused`	Pause the schedule specified for the `-sched` qualifier. Valid values are: • `yes` • `no`
`-noSched`	Unassigns the protection schedule.
`-spOwner`	(Not applicable to thin clones) Specify the default owner of the LUN. Valid values are: • `spa` • `spb`
`-fastvpPolicy`	(Not applicable to thin clones) Specify the FAST VP tiering policy for the LUN. This policy defines both the initial tier placement and the ongoing automated tiering of data during data relocation operations. Valid values (case-insensitive): • `startHighThenAuto` (default)—Sets the initial data placement to the highest-performing drives with available space, and then relocates portions of the storage resource's data based on I/O activity. • `auto`—Sets the initial data placement to an optimum, system-determined setting, and then relocates portions of the storage resource's data based on the storage resource's performance statistics such that data is relocated among tiers according to I/O activity. • `highest`—Sets the initial data placement and subsequent data relocation (if applicable) to the highest-performing drives with available space. • `lowest`—Sets the initial data placement and subsequent data relocation (if applicable) to the most cost-effective drives with available space.
`-lunHosts`	Specify a comma-separated list of hosts with access to the LUN.

Qualifier	Description
`-hlus`	Specifies the comma-separated list of Host LUN identifiers to be used by the corresponding hosts which were specified in the `-lunHosts` option. The number of items in the two lists must match. However, an empty string is a valid value for any element of the Host LUN identifiers list, as long as commas separate the list elements. Such an empty element signifies that the system should automatically assign the Host LUN identifier value by which the corresponding host will access the LUN. If not specified, the system will automatically assign the Host LUN identifier value for every host specified in the `-lunHosts` argument list.
`-snapHosts`	Specify 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` • `no` **Note** This value must be `no` for a thin clone.
`-ioLimit`	Specify the name of the host I/O limit policy to be applied.
`-noIoLimit`	Specify the removal of an applied host I/O limit policy.
`-dataReduction`	(Not applicable to thin clones) Specify whether data reduction is enabled for the LUN. Valid values are: • `yes` • `no` **Note** Data reduction is available for thin LUNs in an All-Flash pool only.
`-advancedDedup`	Specify whether advanced deduplication is enabled for this LUN. This option is available only after data reduction has been enabled. An empty value indicates that advanced deduplication is not supported on the LUN. Valid values are: • `yes` • `no` (default) **Note** Advanced deduplication is available on Unity All-Flash 450F, 550F, and 650F systems only.

Example

The following command updates LUN lun_1 with 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> | -name <value>} delete [-deleteSnapshots {yes | no}] [-async]`

Object qualifiers

Qualifier	Description
-id	Type the ID of the LUN to delete.
-name	Type the name of the LUN to delete.

Action qualifiers

Qualifier	Description
-deleteSnapshots	Specify that snapshots of the LUN can be deleted along with the LUN itself. Valid values are: • 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.
```

Refresh thin clones of a LUN

(Applies to thin clones only) Refresh a LUN's thin clone. This updates the thin clone's data with data from the specified source snapshot and re-parents the thin clone to that snapshot.

Format

```
/stor/prov/luns/lun {-id <value> | -name <value>} refresh [-async] {-source <value> | -sourceName <value>} [-copyName <value>] [-force]
```

Object qualifiers

Qualifier	Description
`-id`	Type the ID of the thin clone to refresh.
`-name`	Type the name of the thin clone to refresh.

Action qualifiers

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-source`	Specify the ID of the snapshot to be used for the thin clone refresh. The snapshot must be part of the base LUN family.
`-sourceName`	Specify the name of the snapshot to be used for the thin clone refresh. The snapshot must be part of the base LUN family.
`-copyName`	Specify the name of the copy to be created before the thin clone refresh.
`-force`	Specify to unconditionally refresh the LUN, even if it has host access configured.

Example

The following command refreshes the thin clone called lun_5_tc with data from snapshot SNAP_2.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/lun
-id lun_5_tc refresh -source SNAP_2 -copyName Backup1
```

```
[Response]
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection

ID = 38654705846
Operation completed successfully.
```

Manage consistency groups

Consistency 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 consistency groups:

Table 111 Consistency group attributes

Attribute	Description
`ID`	ID of the consistency group.
`Name`	Name of the consistency group.
`Description`	Brief description of the consistency group.
`Type`	Type of consistency group. Value is one of the following (case insensitive): • `Primary` • `Thin clone` (**tc** when used with the `-create` command.)
`Base storage resource`	(Applies to thin clones only) ID of the base consistency group for the thin clone.
`Source`	(Applies to thin clones only) ID of the source snapshot for the thin clone.
`Original parent`	(Applies to thin clones only) ID of the parent consistency group for the thin clone.
`Health state`	Health state of the consistency group. The health state code appears in parentheses. Value is one of the following: • `OK (5)`—The 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. ■ 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.

Table 111 Consistency group attributes (continued)

Attribute	Description
	■ 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. ■ 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.
`Total pool space preallocated`	Space reserved from the pool by all associated LUNs for future needs to make writes more efficient. Equal to the sum of all the `sizePreallocated` values of each LUN in the group. The pool may be able to reclaim some of this space if pool space is running low.
`Total pool space used`	Total pool space used in the pool for all the associated LUNs, their snapshots or thin clones, and overhead.
`Thin provisioning enabled`	Identifies 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.
`Data Reduction enabled`	Identifies whether data reduction is enabled. Valid values are: • `yes` • `no` • `mixed`—Indicates that some of the LUNs in the consistency group have data reduction enabled, while some LUNs do not have data reduction enabled. **Note** Data reduction is available for thin LUNs in an All-Flash pool only.

Table 111 Consistency group attributes (continued)

Attribute	Description
`Advanced deduplication enabled`	Identifies whether advanced deduplication is enabled. This option is available only after data reduction has been enabled. An empty value indicates that advanced deduplication is not supported for the LUN in the consistency group. Valid values are: - `yes` - `no` (default) **Note** Advanced deduplication is available on Unity All-Flash 450F, 550F, and 650F systems only.
`Total non-base size used`	(Applies to standard consistency groups only) Quantity of storage used for the snapshots and thin clones associated with this consistency group.
`Total family size used`	(Applies to standard consistency groups only) Quantity of storage used for the whole consistency group family.
`Snapshot count`	Number of snapshots created on the resource.
`Family snapshot count`	(Applies to standard consistency groups only) Number of snapshots created in the consistency group family, including all derivative snapshots.
`Family thin clone count`	(Applies to standard consistency groups only) Number of thin clones created in the consistency group family, including all derivative thin clones.
`Protection schedule`	ID of a protection schedule applied to the consistency group. View protection schedules on page 106 explains how to view the IDs of the schedules on the system.
`Protection schedule paused`	Identifies 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`	Identifies whether the storage resource is a destination for a replication session (local or remote). Valid values are: - `yes` - `no`

Table 111 Consistency group attributes (continued)

Attribute	Description
`Creation time`	Time the consistency group was created.
`Last modified time`	Time the consistency group was last modified.
`FAST VP policy`	FAST VP tiering policy for the consistency group. This policy defines both the initial tier placement and the ongoing automated tiering of data during data relocation operations for each LUN in the consistency group. Valid values (case-insensitive): • `startHighThenAuto` (default)—Sets the initial data placement to the highest-performing drives with available space, and then relocates portions of the storage resource's data based on I/O activity. • `auto`—Sets the initial data placement to an optimum, system-determined setting, and then relocates portions of the storage resource's data based on the storage resource's performance statistics such that data is relocated among tiers according to I/O activity. • `highest`—Sets the initial data placement and subsequent data relocation (if applicable) to the highest-performing drives with available space. • `lowest`—Sets the initial data placement and subsequent data relocation (if applicable) to the most cost-effective drives with available space. • `Mixed`—Value when the LUNs in the consistency group use different FAST VP policies.
`FAST VP distribution`	Percentage of the resource assigned to each tier. The format is: `<tier_name>:<value>%` where: • `<tier_name>` is the name of the storage tier. • `<value>` is the percentage of storage in that tier.

Create a consistency group

Create a consistency group.

Format

```
/stor/prov/luns/group create [-async] -name <value> [-descr
<value>] [-type {primary | tc { -source <value> | -sourceName
<value> } }] [-sched <value> [-schedPaused {yes | no}]] [-
replDest {yes | no}]
```

Action qualifiers

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-name`	Type the name of the consistency group.

Qualifier	Description
	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 consistency group.
`-type`	Specify the type of consistency group. Valid values are (case insensitive): • `primary` (default) • `tc`
`-source`	(Applies to thin clones only) Specify the ID of the source snapshot to use for thin clone creation.
`-sourceName`	(Applies to thin clones only) Specify the name of the source snapshot to use for thin clone creation.
`-sched`	Type the ID of a protection schedule to apply to the consistency group. View protection schedules on page 106 explains how to view the IDs of the schedules on the system.
`-schedPaused`	Specify whether to pause the protection schedule specified for –`sched`. Valid values are: • `yes` • `no` (default)
`-replDest`	(Not applicable when creating a thin clone) Specifies whether the resource is a replication destination. Valid values are: • `yes` • `no` (default)

Example

The following command creates a consistency group with these settings:

- Name is GenericStorage01.
- Description is “MyStorage.”
- Uses protection schedule SCHD_1.

The storage resource receives the ID 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.
```

Example 2

The following command creates a thin clone with these settings:

- Name is MyFC.
- Source is SNAP_1.

The storage resource receives the ID group_2:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/
group create name "MyFC" -descr "My FC" -type tc -sourceName SNAP_1
```

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

ID = group_1
Operation completed successfully.
```

View consistency groups

Display the list of existing consistency groups.

Format

```
group [{-id <value> | -name <value> | -type {primary | tc [{-
originalParent <value> | -originalParentName <value> | -source
<value> | -sourceName <value> | -baseRes <value> | -baseResName
<value>}]}}] show
```

Object qualifiers

Qualifier	Description
`-id`	Type the ID of a consistency group.
`-name`	Type the name of a consistency group.
`-type`	Identifies the type of resources to display. Valid values are (case insensitive): • `primary` • `tc`
`-originalParent`	(Applies to thin clones only) Type the ID of a parent consistency group by which to filter thin clones.
`-originalParentName`	(Applies to thin clones only) Type the name of a parent consistency group by which to filter thin clones.
`-source`	(Applies to thin clones only) Type the ID of a source snapshot by which to filter thin clones.
`-sourceName`	(Applies to thin clones only) Type the name of a source snapshot by which to filter thin clones.
`-baseRes`	(Applies to thin clones only) Type the ID of a base consistency group by which to filter thin clones.
`-baseResName`	(Applies to thin clones only) Type the name of a base consistency group by which to filter thin clones.

Example

The following command display details about the consistency groups and thin clones 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 Consistency group
       Type                                  = Primary
       Base storage resource                 =
       Source                                =
       Original parent                       =
       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 pool space preallocated         = 4292853760 (3.9G)
       Total Pool Space Used                 = 9128919040 (8.5G)
       Total protection size used            = 0
       Snapshot count                        = 0
       Compression enabled                   = yes
       Data Reduction enabled                = yes
       Advanced deduplication enabled        = yes
       Total current allocation              = 10737418240 (10G)
       Protection schedule                   = SCHD_1
       Protection schedule paused            = no
       LUNs access hosts                     = 1014, 1015
       Snapshots access hosts                = 1016(mixed)
       Replication destination               = no
       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%

2:     ID                                    = group_2
       Name                                  = MyLUNGroupFC
       Description                           = My Consistency group
       Type                                  = Thin clone
       Base storage resource                 = group_1
       Source                                = snap_1
       Original parent                       = group_1
       Health state                          = OK (5)
       Health details                        = "The component is operating normally.  No
action is required."
       Total capacity                        = 107374182400 (100G)
       Thin provisioning enabled             = yes
       Total current allocation              =
       Total pool space preallocated         =
       Total Pool Space Used                 =
       Total protection size used            =
       Total non-base size used              = 0
       Total family size used                = 0
       Snapshot count                        = 0
       Compression enabled                   = no
       Data Reduction enabled                = no
       Advanced deduplication enabled        = no
       Protection schedule                   = SCHD_1
       Protection schedule paused            = no
```

```
        LUNs access hosts                     = 1014, 1015
        Snapshots access hosts                =
        Replication destination               = no
        Creation time                         = 2012-12-21 12:55:32
        Last modified time                    = 2013-01-15 10:31:56
        FAST VP policy                        = mixed
        FAST VP distribution                  =
```

Change consistency groups

Change the settings for a consistency group.

Format

```
/stor/prov/luns/group {-id <value> | -name <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}] [-dataReduction {yes [-advancedDedup {yes | no}] | no} ]
```

Object qualifiers

Qualifier	Description
-id	Type the ID of the consistency group to change.
-name	Type the name of the consistency group to change.

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.
-name	Type the name of the consistency group.
-descr	Type a brief description of the consistency group.
-sched	Type the ID of the schedule to apply to the consistency group. View protection schedules on page 106 explains how to view the IDs of the schedules on the system.
-schedPaused	Pause the schedule specified for the -sched qualifier. Valid values are: • yes • no (default)
-noSched	Unassign the protection schedule.
-lunHosts	Specify a comma-separated list of hosts with access to the LUN.
-snapHosts	Specify a comma-separated list of hosts with access to snapshots of the LUN.
-replDest	Specify whether the resource is a replication destination. Valid values are: • yes

Qualifier	Description
	- no (default) **Note** This value must be no for a thin clone.
-fastvpPolicy	(Cannot be changed for thin clones) Specify the FAST VP tiering policy for the consistency group. This policy defines both the initial tier placement and the ongoing automated tiering of data during data relocation operations. Valid values (case-insensitive): - startHighThenAuto (default)—Sets the initial data placement to the highest-performing drives with available space, and then relocates portions of the storage resource's data based on I/O activity. - auto—Sets the initial data placement to an optimum, system-determined setting, and then relocates portions of the storage resource's data based on the storage resource's performance statistics such that data is relocated among tiers according to I/O activity. - highest—Sets the initial data placement and subsequent data relocation (if applicable) to the highest-performing drives with available space. - lowest—Sets the initial data placement and subsequent data relocation (if applicable) to the most cost-effective drives with available space.
-dataReduction	(Cannot be changed for thin clones) Specify whether data reduction is enabled for LUNs in this consistency group. Valid values are: - yes - no **Note** Data reduction is available for thin LUNs in an All-Flash pool only.
-advancedDedup	Specify whether advanced deduplication is enabled for LUNs in this consistency group. This option is available only after data reduction has been enabled. An empty value indicates that advanced deduplication is not supported for LUNs in this consistency group. Valid values are: - yes - no (default) **Note** Advanced deduplication is available on Unity All-Flash 450F, 550F, and 650F systems only.

Example

The following command updates the consistency 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 consistency groups

Delete a consistency group.

Note

Deleting a consistency group removes all LUNs and data associated with the consistency group from the system. After a consistency group is deleted, you cannot restore the data from snapshots. Back up the data from the consistency group before deleting it.

Format

/stor/prov/luns/group {-id *<value>* | -name *<value>* } delete -id *<value>* [-async]

Object qualifiers

Qualifier	Description
-id	Type the ID of the consistency group to delete.
-name	Type the name of the consistency group to delete.

Action qualifier

Qualifier	Description
-deleteSnapshots	Specify that snapshots of the LUN can be deleted along with the LUN itself. Valid values are: • yes • no (default)
-async	Run the operation in asynchronous mode.

Example

The following command deletes LUN consistency 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.
```

Refresh thin clones of a consistency group

(Applies to thin clones only) Refresh a consistency group's thin clone. This updates the thin clones' data with data from the specified source snapshot and re-parents the thin clone to that snapshot.

Format

```
/stor/prov/luns/group {-id <value> | -name <value>} refresh [-async] {-source <value> | -sourceName <value>} [-copyName
<value>] [-force]
```

Object qualifiers

Qualifier	Description
-id	Type the ID of the consistency group to refresh.
-name	Type the name of the consistency group to refresh.

Action qualifiers

Qualifier	Description
-async	Run the operation in asynchronous mode.
-source	Specify the ID of the snapshot to be used for thin clone refresh. The snapshot must be part of the base consistency group family.
-sourceName	Specify the name of the snapshot to be used for thin clone refresh. The snapshot must be part of the base consistency group family.
-copyName	Specify the name of the copy to be created before the thin clone refresh.
-force	Unconditionally refreshes the consistency group, even if the storage resource has host access configured.

Example

The following command refreshes the thin clone called group_2_tc with data from snapshot SNAP_10.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/
group -id group_2_tc refresh -source SNAP_10 -copyName Backup1
```

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

```
ID = 38654705846
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.

Note

You cannot create an NFS datastore on a NAS server that uses IP multi-tenancy.

The following table lists the attributes for NFS datastores:

Table 112 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. • `OK_BUT (7)`—NFS datastore is working, but one or both of the following may have occurred: ▪ The storage resource is being initialized or deleted. ▪ The datastore on this storage resource is running out of space. Allocate more storage space to the storage resource. • `Degraded/Warning (10)`—Working, but one or more of the following may have occurred: ▪ One or more of its storage pools are degraded. ▪ A replication session for the storage resource is 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. • `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. • `Major failure (20)` —One or both of the following may have occurred:

Table 112 NFS datastore attributes (continued)

Attribute	Description
	■ 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. ● `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 file system. The file system ID is displayed for some metrics commands. Use this ID to correlate metrics output with the associated NFS datastore.
`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.
`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.
`Host I/O size`	Typical write I/O size from the host to VMware datastore. This setting is used to match the storage block size to the I/O of the primary application using the VMware datastore, which can optimize IO performance. Host I/O size is only configurable at creation time. Valid values are: ● `8K` ● `16K` ● `32K` ● `64K` ● `Exchange 2007 (8K)` ● `Exchange 2010 (32K)` ● `Exchange 2013 (32K)` ● `Oracle (8K)` ● `SQL Server (8K)`

Table 112 NFS datastore attributes (continued)

Attribute	Description
	- VMware Horizon VDI (8K) - SharePoint (32K) - SAP (8K)
Thin provisioning enabled	Identifies 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.
Data Reduction enabled	Identifies whether data reduction is enabled for this resource. Valid values are: - yes - no (default) **Note** Data reduction is available for thin file systems in an All-Flash pool only. The thin file systems must have been created on Unity systems running version 4.2.x or later.
Data Reduction space saved	Total space saved (in gigabytes) for this resource by using data reduction. **Note** Data reduction is available for thin file systems in an All-Flash pool only. The thin file systems must have been created on Unity systems running version 4.2.x or later.
Data Reduction percent	Total percentage saved for the resource by using data reduction. **Note** Data reduction is available for thin file systems in an All-Flash pool only. The thin file systems must have been created on Unity systems running version 4.2.x or later.
Data Reduction ratio	Ratio of the total storage used before data reduction and after data reduction for this resource.

Table 112 NFS datastore attributes (continued)

Attribute	Description
	Note Data reduction is available for thin file systems in an All-Flash pool only. The thin file systems must have been created on Unity systems running version 4.2.x or later.
`Advanced deduplication enabled`	Identifies whether advanced deduplication is enabled for this resource. This option is available only after data reduction has been enabled. An empty value indicates that advanced deduplication is not supported on the resource. Valid values are: • `yes` • `no` (default) **Note** The thin file systems must be created on a Unity system running version 4.2.x or later. Advanced deduplication is available on Unity All-Flash 450F, 550F, and 650F systems only.
`Current allocation`	If enabled, the quantity of primary storage currently allocated through thin provisioning.
`Minimum size allocated`	(Displays for file systems created on a Unity system running OE version 4.1.) Indicates the minimum quantity of primary storage allocated to the NFS datastore through thin provisioning. File shrink operations cannot decrease the file system size lower than this value.
`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.
`Protection schedule paused`	Identifies whether an applied protection schedule is currently paused. Value is yes or no.
`FAST VP policy`	FAST VP tiering policy for the NFS datastore. This policy defines both the initial tier placement and the ongoing automated tiering of data during data relocation operations. Valid values (case-insensitive): • `startHighThenAuto` (default)—Sets the initial data placement to the highest-performing drives with available space, and then relocates portions of the storage resource's data based on I/O activity. • `auto`—Sets the initial data placement to an optimum, system-determined setting, and then relocates portions of the storage resource's data based on the storage resource's

Table 112 NFS datastore attributes (continued)

Attribute	Description
	performance statistics such that data is relocated among tiers according to I/O activity. • `highest`—Sets the initial data placement and subsequent data relocation (if applicable) to the highest-performing drives with available space. • `lowest`—Sets the initial data placement and subsequent data relocation (if applicable) to the most cost-effective drives with available space.
`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. • `<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.
`Read-only hosts`	ID of each host that has read-only permission to the NFS datastore and its snapshots.
`Read/write hosts`	ID of each host that has read and write permissions 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.
`ESX mount protocol`	Specifies which NFS protocol to use to register the datastore on the ESXi host. Valid values are: • `NFSv3` (default) • `NFSv4`

Table 112 NFS datastore attributes (continued)

Attribute	Description
`Minimum security`	The minimum security option that must be provided by a client in order to have a successful NFS mount operation. Valid values are: • `sys`—No server-side authentication (server relies on NFS client authentication). This is the default setting when there is no configured secure NFS for the NAS server. It is also the default when NFS Secure is enabled without NFSv4 for the NAS server. Also known as AUTH_SYS security. • `krb5`—Kerberos v5 authentication. This is the default value when secure NFSv4 is configured for the NAS server
`NFS owner username`	Default owner of the NFS share associated with the datastore. For NFSv3 or NFSv4 protocols without Kerberos configured, the default owner is `root`.
`Replication type`	Indicates in which asynchronous replication this file system is participating. Valid values are: • `none` • `local` • `remote`
`Synchronous replication type`	Indicates in which synchronous replication this file system is participating. Valid values are: • `none` • `remote`
`Replication destination`	Identifies whether the storage resource is a destination for a replication session (local or remote). Valid values are: • `yes` • `no`
`Creation time`	The time the resource was created.
`Last modified time`	The time the resource was last modified.
`Pool full policy`	Policy to follow when the pool is full and a write to the NFS datastore is attempted. This attribute enables you to preserve snapshots on the NFS datastore when a pool is full. Values are: • `Delete All Snaps` (default for thick file systems)—Delete snapshots associated with the NFS datastore when the pool reaches full capacity. • `Fail Writes` (default for thin file systems)—Fail write operations to the NFS datastore when the pool reaches full capacity. **Note** This attribute is only available for existing NFS datastores. You cannot specify this attribute when creating an NFS datastore.

Table 112 NFS datastore attributes (continued)

Attribute	Description
`Minimum size`	The estimated minimum size that the file system can be shrunk to.
`Reclaimable size`	The estimated size reclaimed by the pool when the file system is shrunk to a specified size.
`Event publishing protocols`	List of file system access protocols enabled for Events Publishing. By default, the list is empty. Valid value is `nfs` (enable Events Publishing for NFS).

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 drive to the pool.
- Configure at least one NAS server to which to associate the NFS datastore.

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> | -serverName
<value>} {pool <value> | -poolName <value>} -size <value> [-
hostIOSize {8K | 16K | 32K | 64K | exchange2007 | exchange2010
| exchange2013 | oracle | sqlServer | vmwareHorizon |
sharePoint | sap}] [-thin {yes | no}] [-dataReduction {yes [-
advancedDedup {yes | no}] | no}] [-minSizeAllocated <value>] [-
sched <value> [-schedPaused {yes | no}]] [-defAccess {ro | root
| na}] [-fastvpPolicy {startHighThenAuto | auto | highest |
lowest}] [-roHosts <value>] [-rwHosts <value>][-rootHosts
<value>] [-naHosts <value>] [-esxMountProtocol {NFSv4 | NFSv3}]
[-minSecurity {sys | krb5}] [-replDest {yes | no}] [-nfsOwner
<value>]}] [-eventProtocols <value>]
```

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. **Note** NFS datastores cannot be created on a NAS server that uses IP multi-tenancy.
-serverName	Type the name of the NAS server that will be the primary NAS server for the NFS datastore. **Note** NFS datastores cannot be created on a NAS server that uses IP multi-tenancy.
-pool	Type the ID of the storage pool that the NFS datastore will use. This value has priority over the value for -poolName. **Note** Value is case-insensitive.
-poolName	Type the name of the storage pool that the NFS datastore will use.
-size	Type the quantity of storage to reserve for the NFS datastore.
-hostIOsize	Type the typical write I/O size from the host to the NFS datastore. Valid values are: • 8K (default) — General purpose 8K • 16K— General purpose 16K • 32K— General purpose 32K • 64K— General purpose 64K • exchange2007— 8K for Microsoft Exchange 2007 applications • exchange2010— 32K for Microsoft Exchange 2010 applications • exchange2013— 32K for Microsoft Exchange 2013 applications • oracle— 8K for Oracle database applications • sqlServer— 8K for Microsoft SQL Server applications

Qualifier	Description
	- vmwareHorizon— 8K for VMware Horizon VDI applications - sharepoint— 32K for Microsoft SharePoint applications - sap— 8K for SAP applications
-thin	Enable thin provisioning on the NFS datastore. Valid values are: - yes - no (default)
-dataReduction	Specify whether data reduction is enabled for this thin NFS datastore. Valid values are: - yes - no (default) **Note** Data reduction is available for thin file systems in an All-Flash pool only. The thin file systems must have been created on Unity systems running version 4.2.x or later.
-advancedDedup	Specify whether advanced deduplication is enabled for this thin NFS datastore. Valid values are: - yes - no (default) **Note** Thin file systems must be created on a Unity system running version 4.2.x or later. Advanced deduplication is available on Unity All-Flash 450F, 550F, and 650F systems only.
-sched	Type the ID of a protection schedule to apply to the storage resource.
-minSizeAllocated	(Option available on a Unity system running OE version 4.1.) Specify the minimum size to allocate for the thin NFS datastore. Automatic and manual file shrink operations cannot decrease the file system size lower than this value. The default value is 3G, which is the minimum thin file system size.
-schedPaused	Specify whether to pause the protection schedule specified for -sched. Valid values are: - yes - no (default)

Qualifier	Description
`-fastvpPolicy`	Specify the FAST VP tiering policy for the NFS datastore. This policy defines both the initial tier placement and the ongoing automated tiering of data during data relocation operations. Valid values (case-insensitive): • `startHighThenAuto` (default) — Sets the initial data placement to the highest-performing drives with available space, and then relocates portions of the storage resource's data based on I/O activity. • `auto` — Sets the initial data placement to an optimum, system-determined setting, and then relocates portions of the storage resource's data based on the storage resource's performance statistics such that data is relocated among tiers according to I/O activity. • `highest` — Sets the initial data placement and subsequent data relocation (if applicable) to the highest-performing drives with available space. • `lowest` — Sets the initial data placement and subsequent data relocation (if applicable) to the most cost-effective drives with available space.
`-defAccess`	Specify the default share access settings for host configurations and for unconfigured hosts that can reach the NFS datastore. Valid values are: • `ro` — Read-only 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` (default) — 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.
`-rwHosts`	Type the ID of each host you want to have read/write access to the datastore. This is only allowed if the NFSv4 ESXi mount protocol is enabled, and the NFS owner is set.
`-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

Qualifier	Description
	brackets after the host ID. For example: ID[IP,IP], where 'ID' is a host configuration ID and 'IP' is an IP address.
`-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.
`-esxMountProtocol`	Type which NFS protocol version will be used to register the NFS datastore on the host. Valid values are: • `NFSv3` (default) • `NFSv4`
`-nfsOwner`	Type the default owner of the NFS share associated with the datastore. This must be specified if the minimum security is set to `krb5` and all hosts passed to the host access list are manually managed. If the passed hosts are all ESXi hosts, this value will be automatically configured to the NFS user configured on the ESXi host. **Note** For NFSv3 or NFSv4 protocols configured without Kerberos, the default owner is `root`.
`-minSecurity`	Type the minimum security option that must be provided by the client in order to have a successful NFS mount operation. Valid values are (in order of lowest to highest security level): • `sys` — No server-side authentication (server relies on NFS client authentication). This is the default setting when there is no configured secure NFS for the NAS server. It is also the default when NFS Secure is enabled without NFSv4 for the NAS server. Also known as AUTH_SYS security. • `krb5`— Kerberos v5 authentication. This is the default value when secure NFSv4 is configured for the NAS server
`-replDest`	Specifies whether the resource is a replication destination. Valid values are: • `yes` • `no` (default)
`-eventProtocols`	Specifies the comma-separated list of file system access protocols enabled for Events Publishing. By default, the list is empty. Valid value is `nfs` (enable Events Publishing for NFS).

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.
- Read-write access to `host1`
- Minimum security level of `krb5`.
- An NFS owner "John"
- Default host access as N/A

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 -rwHosts host1 -esxMountProtocol NFSv4
-minSecurity krb5 -nfsOwner john -defAccess na
```

```
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 or name.

Format

```
/stor/prov/vmware/nfs [ {-id <value> | -name <value>} [-
shrinkToSize <value>]] show
```

Object qualifier

Qualifier	Description
`-id`	ID of the VMware NFS file system.
`-name`	Name of 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 -detail

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


1:    ID                             = res_22
      Name                           = NFSDatastore3
      Description                    =
      Health state                   = OK (5)
      Health details                 = "The component is operating
normally. No action is required."
      File system                    = fs_15
      Server                         = nas_8
      Storage pool ID                = pool_2
      Storage pool                   = Pool 2
      Format                         = UFS64
      Size                           = 1099511627776 (1.0T)
      Size used                      = 312623013888 (291.1G)
      Maximum size                   = 281474976710656 (256.0T)
      Host I/O Size                  = 8K
      Thin provisioning enabled      = yes
      Compression enabled            = yes
      Compression space saved        = 272193552384 (253.5G)
      Compression percent            = 61%
      Compression ratio              = 2.6:1
      Data Reduction enabled         = yes
      Data Reduction space saved     = 272193552384 (253.5G)
      Data Reduction percent         = 61%
      Data Reduction ratio           = 2.6:1
      Advanced deduplication enabled = no
      Current allocation             = 116501004288 (108.5G)
      Preallocated                   = 176802226176 (164.6G)
      Total Pool Space Used          = 174848221184 (162.8G)
      Minimum size allocated         = 0
      Protection size used           = 46267621376 (43.0G)
      Snapshot count                 = 4
      Protection schedule            = snapSch_1
      Protection schedule paused     = no
      Local path                     = /
      Export path                    = 10.245.23.62:/NFSDatastore3
      Default access                 = root
      Read-only hosts                =
      Read/write hosts               =
      Root hosts                     = Host_1
      No access hosts                =
      ESX mount protocol             = NFSv3
      Minimum security               = sys
      NFS owner username             =
      Replication type               = local
      Synchronous replication type   = none
      Replication destination        = no
      Deduplication enabled          =
      Creation time                  = 2018-08-30 18:38:44
      Last modified time             = 2018-08-30 18:38:44
      Minimum size                   =
      Reclaimable size               =
      Pool Full policy               = Fail Writes
      Event publishing protocols     =
```

Example 2

The following command lists details about the vmware_1 NFS datastores with a 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.

Format

/stor/prov/vmware/nfs {-id *<value>* | -name *<value>*} set [-async] –descr *<value>* -size *<value>* [-minSizeAllocated *<value>*] [-dataReduction {yes [-advancedDedup {yes | no}] | no}] [{-sched *<value>* | noSched} [-schedPaused {yes | no}]] [-fastvpPolicy {startHighThenAuto | auto | highest | lowest}] [-defAccess {ro | root | na}] [-roHosts *<value>*] [-rwHosts *<value>*] [-rootHosts *<value>*] [-naHosts *<value>*] [-esxMountProtocol {NFSv4 | NFSv3}] [-minSecurity {sys | krb5}] [-replDest {yes | no}] [-poolFullPolicy {deleteAllSnaps | failWrites}] [-eventProtocols *<value>*]

Object qualifier

Qualifier	Description
-id	Type the ID of the NFS datastore to change.
-name	Type the name 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.

Qualifier	Description
`-minSizeAllocated`	(Option available on a Unity system running OE version 4.1.) Specify the minimum size to allocate for the thin NFS datastore. Automatic and manual file shrink operations cannot decrease the file system size lower than this value. The default value is 3G, which is the minimum thin file system size.
`-dataReduction`	Specify whether data reduction is enabled on the thin NFS datastore. Valid values are: • `yes` • `no` **Note** Data reduction is available for thin file systems in an All-Flash pool only. The thin file systems must have been created on Unity systems running version 4.2.x or later.
`-advancedDedup`	Specify whether advanced deduplication is enabled on the thin NFS datastore. Valid values are: • `yes` • `no` **Note** Thin file systems must be created on a Unity system running version 4.2.x or later. Advanced deduplication is available on Unity All-Flash 450F, 550F, and 650F systems only.
`-sched`	Type the ID of the schedule to apply to the datastore.
`-noSched`	Unassigns the protection schedule.
`-fastvpPolicy`	Specify the FAST VP tiering policy for the NFS datastore. This policy defines both the initial tier placement and the ongoing automated tiering of data during data relocation operations. Valid values (case-insensitive): • `startHighThenAuto` (default)—Sets the initial data placement to the highest-performing drives with available space, and then relocates portions of the storage resource's data based on I/O activity. • `auto`—Sets the initial data placement to an optimum, system-determined setting, and then relocates portions of the storage resource's data based on the storage resource's performance statistics such that data is relocated among tiers according to I/O activity. • `highest`—Sets the initial data placement and subsequent data relocation (if applicable) to the highest-performing drives with available space.

Qualifier	Description
	• `lowest`—Sets the initial data placement and subsequent data relocation (if applicable) to the most cost-effective drives with available space.
`-schedPaused`	Pause the schedule specified for the `-sched` qualifier. Valid values are: • `yes` • `no`
`-defAccess`	Specify the default share access settings for host configurations and for unconfigured hosts who can reach the datastore. Valid values are: • `ro`—Read-only 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.
`-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. `-roHosts`
`-rwHosts`	Type the ID of each host you want to have read/write access to the datastore. This is only allowed if the NFSv4 ESXi mount protocol is enabled, and the NFS owner is set.
`-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.
`-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.
`-esxMountProtocol`	Type which NFS protocol version will be used to register the NFS datastore on the host. Valid values are:

Qualifier	Description
	- `NFSv3` (default) - `NFSv4`
`-minSecurity`	Type the minimum security option that must be provided by the client in order to have a successful NFS mount operation. Valid values are (in order of lowest to highest security level): - `sys`—No server-side authentication (server relies on NFS client authentication). This is the default setting when there is no configured secure NFS for the NAS server. It is also the default when NFS Secure is enabled without NFSv4 for the NAS server. Also known as AUTH_SYS security. - `krb5`—Kerberos v5 authentication.
`-replDest`	Specifies whether the resource is a replication destination. Valid values are: - `yes` - `no`
`-poolFullPolicy`	Specifies the policy to follow when the pool is full and a write to the NFS datastore is attempted. This attribute enables you to preserve snapshots on the NFS datastore when a pool is full. Values are: - `deleteAllSnaps`—Delete snapshots associated with the NFS datastore when the pool reaches full capacity. - `failWrites`—Fail write operations to the NFS datastore when the pool reaches full capacity.
`-eventProtocols`	Specifies the comma-separated list of file system access protocols enabled for Events Publishing. By default, the list is empty. Valid value is `nfs` (enable Events Publishing for NFS).

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 a VMware 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> | -name <value>} delete [-deleteSnapshots {yes | no}] [-async]
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the VMware NFS datastore to delete.
`-name`	Type the name of the VMware NFS datastore to delete.

Action qualifier

Qualifier	Description
`-deleteSnapshots`	Specifies that the resource's snapshots should also be deleted. Valid values are: • yes • no (default)
`-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 File System (VMFS) datastores provide block storage for ESXi hosts. VMFS datastores appear to ESXi hosts as LUNs, to which the hosts connect through Fibre Channel (FC) or the iSCSI protocol. You can provision and manage VMFS datastores and view details about each VMFS datastore on the system, such as their storage capacity and health.

Table 113 VMFS datastore attributes

Attribute	Description
`ID`	ID of the VMFS datastore.

Table 113 VMFS datastore attributes (continued)

Attribute	Description
`LUN`	Logical unit number (LUN) ID of the VMFS datastore.
`Name`	Name of the VMFS datastore.
`Description`	Brief description of the VMFS datastore.
`Type`	Specifies the type of the VMFS datastore. Value is one of the following (case insensitive): • `Primary` • `Thin clone` (**tc** when used with the `-create` command.)
`Base storage resource`	(Applies to thin clones only) ID of the base VMFS datastore for the thin clone.
`Source`	(Applies to thin clones only) ID of the source snapshot of the thin clone.
`Original parent`	(Applies to thin clones only) ID of the parent VMFS datastore for the thin clone.
`Health state`	Health state of the VMFS datastore. The health state code appears in parentheses. Value is one of the following: • `OK (5)`—Datastore is operating normally. • `Degraded/Warning (10)`—Working, but one or more of the following may have occurred: ■ Its storage pool is 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. • `Minor failure (15)`—One or both of the following may have occurred: ■ Its storage pool has failed. ■ The associated iSCSI node has failed. • `Major failure (20)`—One or both of the following may have occurred: ■ Datastore is unavailable. ■ Its associated storage pool has failed. • `Critical failure (25)`—One or more of the following may have occurred: ■ Its storage pool is 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.

Table 113 VMFS datastore attributes (continued)

Attribute	Description
	- Non-recoverable error (30)—One or both of the following may have occurred: - Its storage pool is 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 datastore uses.
Size	Quantity of storage reserved for primary data.
Maximum size	Maximum size to which you can increase the primary storage capacity.
AU size	The size of the allocation unit in kilobytes. Valid values are: - 8 - 16 - 32 - 64
Thin provisioning enabled	Identifies whether thin provisioning is enabled. Valid values are: - yes - no (default) 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.
Data Reduction enabled	Identifies whether data reduction is enabled. Valid values are: - yes - no **Note** Data reduction is available for thin LUNs in an All-Flash pool only.

Table 113 VMFS datastore attributes (continued)

Attribute	Description
Data Reduction space saved	Total space saved (in gigabytes) by using data reduction. **Note** Data reduction is available for thin LUNs in an All-Flash pool only.
Data Reduction percent	Total storage percentage saved by using data reduction. **Note** Data reduction is available for thin LUNs in an All-Flash pool only.
Data Reduction ratio	Ratio between data without data reduction and data after data reduction savings. **Note** Data reduction is available for thin LUNs in an All-Flash pool only.
Advanced deduplication enabled	Identifies whether advanced deduplication is enabled. This option is available only after data reduction has been enabled. An empty value indicates that advanced deduplication is not supported on the storage resource. Valid values are: • yes • no (default) **Note** Advanced deduplication is available on Unity All-Flash 450F, 550F, and 650F systems only.
Current allocation	If thin provisioning is enabled, the quantity of primary storage currently allocated through thin provisioning.
Non-base size used	(Applies to standard VMFS datastores only) Quantity of the storage used for the snapshots and thin clones associated with this datastore.
Family size used	(Applies to standard VMFS datastores only) Quantity of the storage used for the whole datastore family.
Snapshot count	Total number of snapshots on the VMFS datastore.
Family snapshot count	(Applies to standard VMFS datastores only) Number of snapshots on the datastore, including all derivative snapshots.
Family thin clone count	Number of thin clones created in the VMFS datastore family, including all derivative thin clones.
Protection schedule	ID of a protection schedule applied to the VMFS datastore .
Protection schedule paused	Indication of whether an applied protection schedule is currently paused.
SP owner	Indicates the default owner of the LUN. Valid values are:

Table 113 VMFS datastore attributes (continued)

Attribute	Description
	- SPA - SPB
Trespassed	Indicates whether the LUN is trespassed to the peer SP. Valid values are: - yes - no
LUN access hosts	List of hosts with access permissions to the VMFS datastore, presented to the hosts as a LUN.
Virtual disk access hosts	Comma-separated list of hosts with access to the associated disks.
Virtual disk host LUN IDs	Comma-separated list of HLUs (Host LUN identifiers) which the corresponding hosts use to access the virtual disks.
Snapshots access hosts	List of hosts with access permissions to the VMFS datastore snapshots.
WWN	World Wide Name of the VMware resource.
Replication destination	Indication of whether the storage resource is a destination for a replication session (local or remote). Valid values are: - 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 tiering policy for the VMFS datastore. This policy defines both the initial tier placement and the ongoing automated tiering of data during data relocation operations. Valid values (case-insensitive): - startHighThenAuto (default)—Sets the initial data placement to the highest-performing drives with available space, and then relocates portions of the storage resource's data based on I/O activity. - auto—Sets the initial data placement to an optimum, system-determined setting, and then relocates portions of the storage resource's data based on the storage resource's performance statistics such that data is relocated among tiers according to I/O activity. - highest—Sets the initial data placement and subsequent data relocation (if applicable) to the highest-performing drives with available space. - lowest—Sets the initial data placement and subsequent data relocation (if applicable) to the most cost-effective drives with available space.

Table 113 VMFS datastore attributes (continued)

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. • `<value>` is the percentage of storage in that tier.
Version	Indicates the VMFS version of the datastore. Valid values are: • 3 • 5 • 6
Block size	Indicates the block size in megabytes. Valid values are: • 1 • 2 • 4 • 8
IO limit	Indicates the identifier of the applied IO limit.
Effective maximum IOPS	The effective maximum IO per second for the VMFS datastore. For VMFS datastores with a density-based IO limit policy, this value is equal to the product of the `Maximum IOPS` and the `Size` of the attached VMFS datastore.
Effective maximum KBPS	The effective maximum KBs per second for the VMFS datastore. For VMFS datastores with a density-based IO limit policy, this value is equal to the product of the `Maximum KBPS` and the `Size` of the attached VMFS datastore.

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 drive to the pool. Refer to the storage pools commands for how to create pools on the system automatically and for how to create custom pools.
- For iSCSI connections, configure at least one iSCSI interface for use by the VMFS datastore. No additional configuration is required in Unisphere for Fibre Channel connections to VMFS datastores.

Format

```
/stor/prov/vmware/vmfs create [-async] -name <value> [-descr
<value>] [-type {primary | tc {-source <value> | -sourceName
<value>}}] [{-pool <value> | -poolName <value>}] [-size
<value>] [-thin {yes | no}] [-sched <value> [-schedPaused {yes
| no}]] [-spOwner {spa | spb}] [-replDest {yes | no}] [-
dataReduction {yes [-advancedDedup {yes | no}] | no}] [-
fastvpPolicy {startHighThenAuto | auto | highest | lowest}] [-
vdiskHosts <value>] [-hlus <value>] [-snapHosts <value>] [-
version {3 -blockSize {1 | 2 | 4 | 8} | 5 | 6}] [-ioLimit
<value>]
```

Action qualifiers

Qualifier	Description
-async	Run the operation in asynchronous mode.
-name	Type a name for the VMFS datastore. **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.
-type	Specify the type of VMFS datastore. Valid values are (case insensitive): • primary (default) • tc
-source	(Applies to thin clones only) Specify the ID of the source snapshot to use for thin clone creation.
-sourceName	(Applies to thin clones only) Specify the name of the source snapshot to use for thin clone creation.
-pool	(Not applicable when creating a thin clone) Type the ID of the storage pool that the VMFS datastore will use. **Note** Value is case-insensitive.
-poolName	(Not applicable when creating a thin clone) Type the name of the storage pool that the VMFS datastore will use.
-size	(Not applicable when creating a thin clone) Type the quantity of storage to reserve for the VMFS datastore.
-thin	(Not applicable when creating a thin clone) Enable thin provisioning on the VMFS datastore. Valid values are: • yes • no (default)
-sched	Type the ID of a protection schedule to apply to the storage resource.
-schedPaused	Specify whether to pause the protection schedule specified for the -sched parameter. Valid values are: • yes • no

Qualifier	Description
-spOwner	(Not applicable when creating a thin clone) Specify the default SP to which the VMware resource will belong. The storage system determines the default value. Valid values are: • spa • spb
-replDest	(Not applicable when creating a thin clone) Specifies whether the resource is a replication destination. Valid values are: • yes • no (default)
-dataReduction	(Not applicable when creating a thin clone) Specify whether to enable or disable data reduction for the VMFS datastore. Valid values are: • yes • no (default)
-advancedDedup	Specify whether to enable or disable advanced deduplication for the VMFS datastore. This option is available only after data reduction has been enabled. Valid values are: • yes • no (default) **Note** Advanced deduplication is available on Unity All-Flash 450F, 550F, and 650F systems only.
-fastvpPolicy	(Not applicable when creating a thin clone) Specify the FAST VP tiering policy for the VMFS datastore. This policy defines both the initial tier placement and the ongoing automated tiering of data during data relocation operations. Valid values (case-insensitive): • startHighThenAuto (default)—Sets the initial data placement to the highest-performing drives with available space, and then relocates portions of the storage resource's data based on I/O activity. • auto—Sets the initial data placement to an optimum, system-determined setting, and then relocates portions of the storage resource's data based on the storage resource's performance statistics such that data is relocated among tiers according to I/O activity. • highest—Sets the initial data placement and subsequent data relocation (if applicable) to the highest-performing drives with available space. • lowest—Sets the initial data placement and subsequent data relocation (if applicable) to the most cost-effective drives with available space.

Qualifier	Description
`-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.
`-hlus`	Specify the comma-separated list of Host LUN identifiers to be used by the corresponding hosts which were specified in the –`vdiskHosts` option. The number of items in the two lists must match. However, an empty string is a valid value for any element of the Host LUN identifiers list, as long as commas separate the list elements. Such an empty element signifies that the system should automatically assign the Host LUN identifier value by which the corresponding host will access the virtual disk. If this option is not specified, the system will automatically assign the Host LUN identifier value for every host specified in the `–vdiskHosts` argument list.
`-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.
`-version`	Type the VMFS version of the datastore. Valid values are: • `3` • `5` (default) • `6`
`-blockSize`	Type the block size in megabytes of the datastore. Valid values are: • `1` • `2` • `4` • `8` (default)
`-ioLimit`	Type the size of the I/O limit to be applied to the VMFS datastores.

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.

Format

```
/stor/prov/vmware/vmfs [{-id <value> | -name <value> | -type
{primary | tc {-baseRes <value> | -baseResName <value> | -
originalParent <value> | -originalParentName <value> | -source
<value> | -sourceName <value>}]}}] show
```

Object qualifier

Qualifier	Description
-id	Type the ID of a VMFS datastore.
-name	Type the name of a VMFS datastore.
-standalone	Displays only VMFS datastores that are not part of a consistency group.
-type	Identifies the type of resources to display. Valid values are (case insensitive): • primary • tc
-baseRes	(Applies to thin clones only) ID of the base VMFS datastore by which to filter thin clones.
-baseResName	(Applies to thin clones only) Name of the base VMFS datastore by which to filter thin clones.
-originalParent	(Applies to thin clones only) ID of the parent VMFS datastore by which to filter thin clones.
-originalParentName	(Applies to thin clones only) Name of the parent VMFS datastore by which to filter thin clones.
-source	(Applies to thin clones only) ID of the source snapshot by which to filter thin clones.
-sourceName	(Applies to thin clones only) Name of the source snapshot by which to filter thin clones.

Example 1

The following command displays details about VMFS datastores and their thin clones :

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/vmfs show -detail

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

1:    ID                             = res_6
      LUN                            = sv_25
      Name                           = VMFS Datastore 1
      Description                    =
      Type                           = Primary
      Base storage resource          = res_6
      Source                         =
      Original parent                =
      Health state                   = OK (5)
      Health details                 = "The component is operating 
normally. No action is required."
      Storage pool ID                = pool_1
      Storage pool                   = Pool 1
      Size                           = 1099511627776 (1.0T)
      Maximum size                   = 70368744177664 (64.0T)
      Thin provisioning enabled      = yes
      Compression enabled            = yes
      Compression space saved        = 267361714176 (249.0G)
      Compression percent            = 57%
      Compression ratio              = 2.3:1
      Data Reduction enabled         = yes
      Data Reduction space saved     = 267361714176 (249.0G)
      Data Reduction percent         = 57%
      Data Reduction ratio           = 2.3:1
      Advanced deduplication enabled = no
      Current allocation             = 172823429120 (160.9G)
      Preallocated                   = 82576048128 (76.9G)
      Total Pool Space Used          = 203844583424 (189.8G)
      Protection size used           = 20820606976 (19.3G)
      Non-base size used             = 20820606976 (19.3G)
      Family size used               = 203844583424 (189.8G)
      Snapshot count                 = 2
      Family snapshot count          = 2
      Family thin clone count        = 0
      Protection schedule            = snapSch_1
      Protection schedule paused     = no
      SP owner                       = SPB
      Trespassed                     = no
      Version                        = 5
      Block size                     = 1
      Virtual disk access hosts      = Host_2
      Host LUN IDs                   = 12
      Snapshots access hosts         =
      WWN                            = 60:06:01:60:09:00:43:00:CB:
38:88:5B:BB:10:5B:09
      Replication destination        = no
      Creation time                  = 2018-08-30 18:34:46
      Last modified time             = 2018-08-30 18:34:46
      IO limit                       =
      Effective maximum IOPS         = N/A
      Effective maximum KBPS         = N/A
```

Example 2

The following command displays details about the thin clones derived from the LUN named sv_2:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/
vmfs -id vmware_2 show
```

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

       ID                     = vmware_2
       LUN                       = sv_2
       Name                   = MyFC
       Description            = My description
       Type                   = Thin clone
       Base storage resource = vmware_1
       Source                 = snap_1
       Original parent        = vmware_1
       Health state           = OK (5)
       Storage pool ID        = pool_2
       Storage pool           = capacity
       Size                   = 107374182400 (100G)
       Protection size used  =
       Non-base 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>* | -name *<value>*} set [-async] [-name *<value>*] [-descr *<value>*] [-size *<value>*] [{-sched *<value>* | -noSched}] [-schedPaused {yes | no}] [-spOwner {spa | spb}] [-replDest {yes | no}] [-dataReduction {yes [-advancedDedup {yes | no}] | no}] [-fastvpPolicy {startHighThenAuto | auto | highest | lowest}] [-vdiskHosts *<value>* [-hlus *<value>*]] [-snapHosts *<value>*] [{-ioLimit *<value>* | -noIoLimit}]

Object qualifier

Qualifier	Description
-id	Type the ID of the VMFS datastore to change.
-name	Type the name 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. 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.

Qualifier	Description
`-descr`	Type a brief description of the VMFS datastore.
`-size`	(Not applicable to thin clones) Type the quantity of storage to allocate for the VMFS datastore.
`-sched`	Type the ID of a protection schedule to apply to the VMFS datastore.
`-noSched`	Unassign the protection schedule.
`-schedPaused`	Specify whether to pause the protection schedule specified for `-sched`. Valid values are: • `yes` • `no`
`-spOwner`	(Not applicable to thin clones) Specify the default SP that owns the datastore. Valid values are: • `spa` • `spb`
`-replDest`	Specifies whether the resource is a replication destination. Valid values are: • `yes` • `no` **Note** This value must be `no` for a thin clone.
`-dataReduction`	(Not applicable to thin clones) Specify whether to enable or disable data reduction for the VMFS datastore. Valid values are: • `yes` • `no`
`-advancedDedup`	Specify whether to enable or disable advanced deduplication for the VMFS datastore. Valid values are: • `yes` • `no` (default) **Note** Advanced deduplication is available on Unity All-Flash 450F, 550F, and 650F systems only.
`-fastvpPolicy`	(Not applicable to thin clones) Specify the FAST VP tiering policy for the VMFS datastore. This policy defines both the initial tier placement and the ongoing automated tiering of data during data relocation operations. Valid values (case-insensitive): • `startHighThenAuto` (default) — Sets the initial data placement to the highest-performing drives with available

Qualifier	Description
	space, and then relocates portions of the storage resource's data based on I/O activity. - `auto` — Sets the initial data placement to an optimum, system-determined setting, and then relocates portions of the storage resource's data based on the storage resource's performance statistics such that data is relocated among tiers according to I/O activity. - `highest` — Sets the initial data placement and subsequent data relocation (if applicable) to the highest-performing drives with available space. - `lowest` — Sets the initial data placement and subsequent data relocation (if applicable) to the most cost-effective drives with available space.
`-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.
`-hlus`	Specify the comma-separated list of Host LUN identifiers to be used by the corresponding hosts which were specified in the –`vdiskHosts` option. The number of items in the two lists must match. However, an empty string is a valid value for any element of the Host LUN identifiers list, as long as commas separate the list elements. Such an empty element signifies that the system should automatically assign the Host LUN identifier value by which the corresponding host will access the virtual disk. If this option is not specified, the system will automatically assign the Host LUN identifier value for every host specified in the `–vdiskHosts` argument list.
`-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.
`-ioLimit`	Type the size of the I/O limit to be applied.
`-noIoLimit`	Specifies that an existing I/O limit applied to the VMFS datastore will be removed.

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.

Note

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> | -name <value>} delete [-
deleteSnapshots {yes | no}] [-async] delete [-deleteSnapshots
{yes | no}] [-async]
```

Object qualifier

Qualifier	Description
-id	Type the ID of the VMFS datastore to delete.
-name	Type the name 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.
```

Refresh thin clones of a VMFS datastore

(Applies to thin clones only) Refresh the thin clone of a VMFS datastore. This updates the thin clone's data with data from the specified source snapshot.

Format

```
/stor/prov/vmware/vmfs {-id <value> | -name <value>} refresh [-async] {-source <value> | -sourceName <value>} -copyName <value> [-force]
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the VMFS datastore.
`-name`	Type the name of the VMFS datastore.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-source`	Specify the ID of the snapshot to be used for the thin clone refresh. The snapshot must be part of the base VMFS datastore family.
`-sourceName`	Specify the name of the snapshot to be used for the thin clone refresh. The snapshot must be part of the base VMFS datastore family.
`-copyName`	Specify the name of the copy to be created before the thin clone refresh.
`-force`	Unconditionally refreshes the VMFS resource, even if the storage resource has host access configured.

Example

The following command refreshes the thin clone called vmware_2_tc with data from snapshot SNAP_2.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/vmfs -id vmware_2_tc refresh -source SNAP_2 -copyName Backup1
```

```
[Response]
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection

ID = 38654705846
Operation completed successfully.
```

Manage VMware protocol endpoints

Protocol Endpoints (PEs) are access points for ESX/ESXi host communication to the storage system. These endpoints establish a datapath on-demand for virtual machines and their respective VVol datastores. I/O from VMs is communicated through the PE to the VVol datastore on the storage system. A single protocol endpoint can multiplex I/O requests from a large number of VM clients to their virtual volumes.

NAS protocol endpoints are created and managed on the storage system and correspond to a specific NFS-based NAS server. It is recommended that you enable at least two NAS servers for VVols, one for each SP, for high availability. A File VVol will be bound to the associated NAS PE every time that VM is powered on. When the VM is powered off, VVols are unbound from the PE.

SCSI protocol endpoints correspond to a specific iSCSI interface or Fibre Channel connection. The Block VVol will be bound to the associated SCSI PE every time that the VM is powered on. When the VM is powered off, the PE is unbound. SCSI protocol endpoints are like LUN mount points that allow I/O access to VVols from the ESXi host to the storage system.

Table 114 Protocol endpoint attributes

Attribute	Description
`ID`	VMware protocol endpoint identifier.
`Name`	Protocol endpoint name.
`Type`	Type of protocol endpoint. Valid values are: - `SCSI` - `NAS`
`VMware UUID`	VMware UUID of the protocol endpoint.
`Export path` (NAS PEs only)	Export path to the PE.
`IP address`	IP address of the NAS server for File PEs.
`WWN`	The World Wide Name for Block PEs.
`Default SP`	Identifier for the preferred SP. Valid values are: - `SPA` - `SPB`
`Current SP`	Identifier for the current SP. Valid values are: - `SPA` - `SPB`
`NAS server`	Identifier of the associated NAS server for NAS PEs.
`VMware NAS PE server` (NAS PEs only)	ID of the corresponding VMware NAS PE server.
`VVol datastore` (NAS PEs only)	ID of the VVol datastore using the PE.
`Host` (SCSI PEs only)	Comma-separated list of identifiers for hosts that use the PE.
`LUN ID`	Logical Unit Number for the protocol endpoint on the host.
`Health state`	Health state.
`Health details`	Additional health information.

View protocol endpoints

Displays a list of existing protocol endpoints and their characteristics.

Format

```
/stor/prov/vmware/pe [-id <value>] show
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the protocol endpoint.

Example

The following example shows the detail for all protocol endpoints on the system.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/pe
show -detail
```

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

1:     ID                   = rfc4122.60060160-
ca30-3c00-962b-87806445241a
       Name                 = scsi_pe_1
       Type                 = SCSI
       VMware UUID          = rfc4122.60060160-
ca30-3c00-962b-87806445241a
       Export path          =
       IP address           =
       WWN                  = 60:06:01:60:CA:30:3C:00:96:2B:
87:80:64:45:24:1A
       Default SP           = SPA
       Current SP           = SPA
       NAS Server           =
       VMware NAS PE server =
       VVol datastore       =
       Host                 = Host_1
       LUN ID               =
       Health state         = OK (5)
       Health details       = "The protocol endpoint is operating
normally. No action is required."
```

Change VMware protocol endpoint

Changes the settings for a VMware protocol endpoint. This command is applicable to SCSI protocol endpoints only.

Format

```
/stor/prov/vmware/pe –id <value> set [-async] –lunid <value>
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the protocol endpoint.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.

Qualifier	Description
	Note Simultaneous commands, regardless of whether they are asynchronous, may fail if they conflict in trying to manage the same system elements.
`-lunid`	Specify the new SCSI LUN ID for this protocol endpoint on the host.

Example

The following command changes the LUN used by the SCSI protocol endpoint.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/pe
set -id rfc4122.d54a64e3-9511-4832-90c3-b2cdfb622a2c set -lunid 5
```

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

ID = rfc4122.d54a64e3-9511-4832-90c3-b2cdfb622a2c
Operation completed successfully.
```

Manage VVol datastores

VVols reside in VVol datastores, also known as storage containers, which are comprised of storage allocations from one or more capability profiles. Capability profiles are built on top of one or more underlying storage pools. You can create VVol datastores based on one or more capability profiles and then allocate a specific amount of space from the capability profile to the VVol datastore.

Each VVol datastore has one or more capability profiles that describe its performance and capacity characteristics, such as drive type, FAST VP tiering policy, and space efficiency policy (thick or thin). These characteristics are derived based on the underlying storage pool. When a virtual volume is created in vSphere, it is assigned a storage policy profile. vSphere filters the compatible and incompatible available VVol datastores (from one or more storage systems) when the VVol is being created based on these profiles. Only VVol datastores that support the storage policy profile are considered compatible storage containers for deploying the VVol.

Table 115 VVol datastore attributes

Attribute	Description
`ID`	VVol datastore identifier.
`Name`	VVol datastore name.
`Description`	VVol datastore description.
`VMware UUID`	VWware UUID of the VVol datastore.
`Type`	Type of VVol datastore. Valid values are: • `File` • `Block`
`Health state`	Health state of the VVol datastore. Value is one of the following:

Table 115 VVol datastore attributes (continued)

Attribute	Description
	• Unknown (0) - Health is unknown. • OK (5) - Operating normally. • OK BUT (7) ■ Storage resource allocation from one or more pools has exceeded the 85% threshold. ■ Storage resource allocation from one or more pools has exceeded the 95% threshold. • Degraded/Warning (10) ■ Pool performance is degraded on one or more of the underlying storage pools for the virtual volume. ■ Storage resource allocation from one or more pools has exceeded the 95% threshold, and the storage resource is oversubscribed. • Major failure (20) ■ The storage resource has failed due to one or more failed storage pools. ■ The storage resource is unavailable due to one or more unavailable servers. ■ The storage resource is unavailable and requires a Storage Integrity Check. • Critical failure (25) - One or more of the underlying storage pools for a virtual volume is offline. • Non-recoverable error (30) - Resource unavailable due to one or more unavailable storage pools.
Health details	Detailed health state for the VVol datastore.
Capability profile	Comma-separated list of identifiers of capability profiles supported by the VVol datastore. Each identifier with a "(Not used)" suffix indicates that this profile can be removed from the VVol datastore.
Storage pool ID	Comma-separated list of identifiers of storage pools used for the VVol datastore.
Total capacity	Total capacity of the VVol datastore.
Total current allocation	Total current allocation of the VVol datastore in all associated storage pools.
Total used capacity	Total used capacity of the VVol datastore.
Creation time	Time when the VVol datastore was created.
Hosts	Hosts that have access to the datastore.
Last modified time	Time when the VVol datastore was last modified.

Create VVol datastores

Create a datastore for VMware VVols.

Format

```
/stor/prov/vmware/vvolds create [-async] -name <value> [-descr
<value>] -cp <value> -size <value> -type { block | file } [-
hosts <value>]
```

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-name`	Type a name for the VVol datastore. **Note** The name may contain alphanumeric values, a hyphen, an underscore, and a period. It cannot start with hyphen or period, and cannot consist only of digits.
`-descr`	Type a brief description for the VVol datastore.
`-cp`	Specify the list of identifiers of capability profiles supported by the VVol datastore.
`-size`	Specify the list of allocation sizes. Specify one allocation for the amount of total space available for VVol provisioning on the VVol datastore for the specified capability profile. If there are multiple capability profiles, the list should include allocation size respective to each capability profile.
`-type`	Specify the VVol datastore type. Valid values are: • `block` • `file`
`-hosts`	Specify the comma-separated list of hosts that will have access to the VVol datastore. For a list of eligible hosts, refer to View host configurations on page 277.

Example

The following command creates a VVol datastore with these settings:

- A VVol datastore name of "Engineering department"
- Associates the "cp_1" and "cp_2" capability profiles with this VVol datastore
- Allocates 10 GBs and 12 GBs from capability profiles cp_1 and cp_2, respectively, to the VVol datastore
- Grants access for "Host_1" and "Host_2" to the datastore

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/
vvolds create -name "Engineering department" -cp cp_1,cp_2 -size 10G,
12G -type file -hosts "Host_1,Host_2"
```

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

```
HTTPS connection

ID = res_1
Operation completed successfully.
```

View VVol datastores

Display a list of existing VVol datastores and their characteristics.

Format

```
/stor/prov/vmware/vvolds [-id <value>] show
```

Object qualifiers

Qualifier	Description
`-id`	Type the ID of the VVol datastore.

Example

The following command displays a list of VVol datastores and their characteristics.

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/vvolds show -detail`

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

1:     ID                        = res_1
       Name                      = Performance
       Description               =
       VMware UUID               = 550e8400-e29b-41d4-
a716-446655440000
       Type                      = Block
       Health state              = OK (5)
       Health details            = "The component is operating
normally. No action is required."
       Capability profile        = cp_1, cp_2 (Not used)
       Storage pool              = pool_1,pool_3
       Total capacity            = 128849018880 (120G)
       Total current allocation = 12884901888 (12G)
       Total used capacity       = 1073741824 (1G)
       Hosts                     = Host_1
       Creation time             = 2015-12-21 12:55:32
       Last modified time        = 2016-01-15 10:31:56

2:     ID                        = res_2
       Name                      = engineering
       Description               =
       VMware UUID               = rfc4122.534e0655-
f5a3-41d7-8124-9d53be5d0c0d
       Type                      = file
       Health state              = OK (5)
       Health details            = "The component is operating
normally. No action is required."
       Capability profile        = cp_1, cp_2
       Storage pool              = pool_1, pool_2
       Total capacity            = 644245094400 (600.0G)
       Total current allocation = 0
       Total used capacity       = 0
       Creation time             = 2015-06-20 01:48:54
       Last modified time        = 2015-06-20 01:48:54
```

Change VVol datastores

Modify an existing VVol datastore.

Format

```
/stor/prov/vmware/vvolds -id <value> set [-async] [-name
<value>] [-descr <value>] [{-addCp <value> -size <value> | -
modifyCp <value> -size <value> | -removeCp <value>}] [-hosts
<value> [-force]]
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the VVol datastore to be modified.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-name`	Type a name for the VVol datastore. **Note** The name may contain alphanumeric values, a hyphen, an underscore, and a period. It cannot start with hyphen or period, and cannot consist only of digits.
`-descr`	Type a new description for the VVol datastore.
`-addCp`	Type the list of identifiers of new capability profiles the VVol datastore will support.
`-modifyCp`	Type the list of identifiers of capability profiles already supported by the VVol datastore and specify the new allocated sizes for each.
`-size`	Specify the list of allocation sizes. Specify one allocation for the amount of total space available for VVol provisioning on the VVol datastore for the specified capability profile. If there are multiple capability profiles, the list should include allocation size respective to each capability profile.
`-removeCp`	Type the list of identifiers of capability profiles you would like to remove from the VVol datastore. **Note** This command can only used on capability profiles that are not currently in use by existing virtual volumes.
`-hosts`	Type the list of comma-separated hosts that will have access to the VVol datastore.
`-force`	Type to unconditionally unbind all virtual volumes that are currently bound to a protocol endpoint associated with a particular host.

Qualifier	Description
	Note If host access is changed or removed for a VVol datastore, the associated protocol endpoints are automatically unbound.

Example

The following command modifies the following settings of a VVol datastore:

- Changes the description of the VVol datastore to "My new description"
- Changes the name of the VVol datastore to "MyNewName"
- Associates the capability profile "cp_1" with VVol datastore "res_1"
- Allocates 10 GBs of space from the pool to capability profile "cp_1"

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/vvolds -id res_1 set -name MyNewName -descr "My new description" -addCp cp_1 -size 10G

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

ID = res_1
Operation completed successfully.
```

Delete VVol datastores

Deletes specified VVol datastores and their associated virtual volumes.

Format

`/stor/prov/vmware/vvolds [-id <value>] delete [-async] [-force { yes | no}]`

Object qualifier

Qualifier	Description
`-id`	Type the ID of the VVol datastore.

Action qualifier

Qualifier	Description
`-force`	Delete the VVol datastore and any of its associated VVols. Valid values are: • `yes` • `no`
`-async`	Run the operation in asynchronous mode.

Example

The following command deletes VVol datastore res_1 as well as its virtual volumes.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/
vvolds -id res_1 delete -force yes
```

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

Operation completed successfully.
```

Manage VVol datastore allocation

Manage the allocation of storage to VVol datastores.

Table 116 VVol datastore allocation attributes

Attribute	Description
`ID`	VVol datastore allocation identifier.
`VVol datastore`	VVol datastore identifier.
`Capability profile`	Identifier of the associated capability profile.
`Storage pool`	Comma-separated list of identifiers of storage pools associated with the capability profile.
`Size`	Amount of total space available for VVol provisioning for a particular capability profile on the VVol datastore.
`Current allocation`	Quantity of primary storage currently allocated for the VVol datastore for VVols provisioned with a particular capability profile on the VVol datastore.
`Size used`	Amount of space used by virtual volumes provisioned with a particular capability profile on the VVol datastore.
`Health state`	Health state of the VVol datastore allocation.
`Health details`	Additional health information.

View VVol datastore allocation details

Displays existing VVol datastore allocations.

Format

```
/stor/prov/vmware/vvolds/alloc {-id <value> | -vvolds <value>
[{-pool <value> | -cp <value>}]} show
```

Object qualifier

Qualifier	Description
`-id`	Type the allocation identifier of the VVol datastore.
`-vvolds`	Type the ID of the VVol datastore.
`-pool`	Type the ID of the storage pool.

Qualifier	Description
`-cp`	Type the ID of the capability profile.

Note

To obtain the ID of the VVol datastore and it's associated pool and capability profile IDs, refer to View VVol datastores on page 506.

Example

The following command shows the allocation details for the VVol datastore "vvol_1" from pool "pool_1", including associated capability profile IDs, current size of the storage pool, and current size allocated to the VVol datastore from the storage pool.

```
uemcli /stor/prov/vmware/vvolds/alloc -vvolds vvolds_1 -pool pool_1
show -detail
```

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

1:      ID                   = cpa_1
        VVol datastore       = res_1
        Capability profile = cp_1
        Storage pool         = pool_1
        Size                 = 128849018880 (120G)
        Current allocation = 12884901888 (12G)
        Size used            = 1073741824 (1G)
        Health state         = OK (5)
        Health details       = "The component is operating normally.
No action is required."
```

Manage VVol objects

Virtual volumes are encapsulations of virtual machine files, virtual disks, and their derivatives. There are several types of VVol objects that correspond to an individual virtual volume, including a VMDK VVol (data VVol), Config VVol, Memory VVol, and Swap VVol.

Table 117 Types of VVols

VMDK (Data) VVol	The VMDK VVol, displayed as **Data** VVol in Unisphere, contains the vDisk file, or the hard disk drive, for the VM.
Config VVol	The **Config** VVol contains settings, configuration, and state information for the VM. This includes .vmx, nvram, and log files.
Memory VVol	The **Memory** VVol contains a complete copy of the VM memory as part of a with-memory VM snapshot.
Swap VVol	The **Swap** VVol is created when VMs are powered on and contain copies of the VM memory pages that are not retained in memory.

Table 118 VVol attributes

Attribute	Description
ID	Virtual volume identifier.
Name	Virtual volume name.
Type	Type of virtual volume. Valid values are: • Data • Config • Memory • Swap • Other
Replica type	Virtual volume replica type. Valid values are: • Base • Prepared Snap • Ready Snap • Fast-Clone
Parent	Identifier of the base/parent virtual volume for the snap, prepared snap, or fast-clone.
Health state	Health state of the virtual volume.
Health details	Additional health information for the virtual volume.
Datastore	Identifier of the datastore associated with the virtual volume.
Storage pool	Identifier of the storage pool that contains the virtual volume.
Capability profile	Identifier of the capability profile associated with the virtual volume.
Policy profile	Name of the VMware vSphere policy profile.
Compliant	Indicates whether the virtual volume is compliant with the VMware vSphere policy profile.
Size	Size of the virtual volume.
Current allocation	Total current allocation of the virtual volume.
Bound to	Comma-separated list of protocol endpoint identifiers to which the virtual volume is bound. An empty value indicates an unbound virtual volume.
Binding details	Binding details of the protocol endpoint to which the virtual volume is bound. • For virtual volumes bound to NFS protocol endpoints, this displays the full NFS paths. • For virtual volumes bound to iSCSI protocol endpoints, this displays the virtual volume iSCSI secondary ID.

Table 118 VVol attributes (continued)

Attribute	Description
	- For unbound virtual volumes, this value is empty.
`Virtual machine`	Identifier of the virtual machine.
`VM hard disk`	Name of the associated VM hard disk.

View VVol objects

Display a list of existing VVol datastores and their characteristics.

Format

```
/stor/prov/vmware/vvol {[-id <value> | [-vm <value>] [-cp
<value>] [-pool <value>] [-datastore <value>] [-pe <value>] [-
parent <value>] [-bound] [-noncompliant] } show
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the virtual volume.
`-vm`	Type the ID of the associated VM for the virtual volume.
`-cp`	Type the ID of the capability profile associated with the virtual volume.
`-pool`	Type the ID of the storage pool that contains the virtual volume.
`-datastore`	Type the ID of the associated VVol datastore.
`-pe`	Type the ID of the protocol endpoint for which you want to see bound virtual volumes.
`-parent`	Type the ID of the parent virtual volume.
`-bound`	Specify in order to display a list of only bound virtual volumes.
`-noncompliant`	Specify in order to display only a list of virtual volumes not compliant with their respective VMware policy profiles.

Example

The following example displays the details of all VVols for the VM with the ID VM_1.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/
vvol -vm VM_1 show -detail
```

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

1:     ID                  = rfc4122.de305d54-75b4-431b-adb2-
eb6b9e546014
       Name                = Hard disk 1
       Type                = Data
       Replica type        = Base
       Parent              =
       Health state       = OK (5)
       Health details     = "The component is operating normally.
No action is required."
       Datastore          = res_1
       Storage pool       = pool_1
       Capability profile = cp_1
       Policy profile     = VMware policy profile
       Compliant          = yes
       Size               = 1073741824 (1G)
       Thin               = yes
       Current allocation = 107374182 (100M)
       Bound to           = NASPE_1
       Binding details    = 192.168.3.3:/vvol1
       Virtual machine    = VM_1
       VM hard disk       = VM Hard Disk 1
```

Delete VVol objects

Deletes the specified existing VVol objects.

Note

Deletion of VVol objects must be exclusively confirmed by the user. The following confirmation message will display:

```
Virtual volume deletion will also unbind and delete associated snapshots
and fast-clones. Do you want to delete the virtual volume?
yes / no:
```

The default in silent mode is `yes`.

Format

`/stor/prov/vmware/vvol -id <value> delete [-async]`

Object qualifier

Qualifier	Description
`-id`	Type the ID of the virtual volume.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.

Example

The following command deletes the virtual volume with the ID naa. 6006016005603c009370093e194fca3f.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/
vvol -id naa.6006016005603c009370093e194fca3f delete
```

```
Virtual volume deletion will also unbind and delete associated
snapshots and fast-clones. Do you want to delete the virtual
volume?
```

```
yes / no:
yes

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

Operation completed successfully.
```

Manage capability profiles

A capability profile is a group of storage capabilities that are applicable for VVol datastores. You must create one or more capability profiles before creating VVol datastores.

Capabilities are automatically derived from the underlying storage pool and are determined by the pool properties. Usage tags are assigned by the storage admin.

There are three ways to profile storage capabilities for a pool:

Table 119 Storage capabilities

Capability name	Description
Service level-based provisioning (physical deployments)	Expected service level for the pool: • Platinum ▪ Single-tiered Flash pool • Gold ▪ Multitiered pool with a mix of Flash and SAS drives ▪ Single-tiered pools with SAS RAID 10 • Silver ▪ Single-tiered pools with SAS RAID 5 or RAID 6 ▪ Multitiered pools with a mix of SAS and NL-SAS • Bronze ▪ Single-tiered pools with NL-SAS ▪ Multitiered pools with a mix of Flash and NL-SAS
Service level-based provisioning (virtual deployments)	Expected service level for a virtual pool: • Gold ▪ Multitiered pool with a mix of Extreme Performance and Performance tiers ▪ Single-tiered Extreme Performance pool • Silver ▪ Multitiered pool with a mix of Extreme Performance, Performance, and Capacity tiers ▪ Multitiered pool with a mix of Performance and Capacity tiers

Table 119 Storage capabilities (continued)

Capability name	Description
	■ Single-tiered Performance pool • Bronze ■ Multitiered pool with a mix of Extreme Performance and Capacity tiers ■ Single-tiered Capacity pool
Usage tags	Usage tags can be applied to capability profiles to designate them and their associated VVol datastores for a particular use. For example, a VVol datastore may be tagged for VVols and VMs that support a particular application. The virtualization administrator and storage administrator should collaborate to define these usage tags.
Storage properties	Supported storage properties include: • Drive type: ■ Extreme Performance [Flash] ■ Performance [SAS] ■ Capacity [NL-SAS] ■ Multitier [mixed] ■ Extreme Multitier [mixed with Flash] • RAID type (physical deployments only): ■ RAID5 ■ RAID6 ■ RAID10 ■ Mixed • FAST Cache (physical deployments only): ■ Enabled ■ Disabled • FAST VP tiering policy: ■ Highest Available Tier ■ Start High then Auto-Tier ■ Auto-Tier ■ Lowest Available Tier • Space Efficiency: ■ Thick ■ Thin

Table 120 Capability profile attributes

Attribute	Description
`ID`	Capability profile identifier.
`Name`	Capability profile name.
`Description`	Capability profile description.
`VMware UUID`	VMware UUID of the capability profile.
`Storage pool`	Associated storage pool identifier.
`Service level`	Service level of the underlying storage pool. Valid values are: • `Platinum` • `Gold` • `Silver` • `Bronze`
`Usage tag`	Comma-separated list of user-defined tags. Each tag is an alphanumeric string value.
`Drive type`	Specifies the drive type of the underlying storage pool. Valid values are: • `CapacityTier` • `PerformanceTier` • `ExtremePerformanceTier` • `MultiTier` • `ExtremeMultiTier`
`RAID level` (physical deployments only)	Specifies the RAID level of the underlying storage pool. Valid values are: • `RAID5` • `RAID10` • `RAID6` • `Mixed`
`FAST Cache` (physical deployments only)	Indicates whether or not FAST Cache is enabled on the underlying storage pool. Valid values are: • `On` • `Off`
`FAST VP policy`	Comma-separated list of FAST VP storage policies for the underlying storage pool. Valid values are: • `Start high then auto-tier` • `Auto-tier` • `Highest available tier`

Table 120 Capability profile attributes (continued)

Attribute	Description
	• `Lowest available tier`
`Space efficiency`	Comma-separated list of available space efficiency policies for the underlying storage pool. Valid values are: • `Thick` • `Thin`
`Health state`	Health state.
`Health details`	Additional health information.

Create a capability profile

Create a capability profile for VVol datastores.

Format

```
/stor/config/cp create [-async] -name <value> [-descr <value>]
-pool <value> [-usageTag <value>]
```

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-name`	Type a name for the capability profile. **Note** The name may contain alphanumeric values, a hyphen, an underscore, and a period. It cannot start with hyphen or period, and cannot consist only of digits.
`-descr`	Type a description for the capability profile.
`-pool`	Specify the identifier of the storage pool the capability profile is based on.
`-usageTag`	Type a comma-separated list of user-specified usage tags. Each tag is an alphanumeric string value.

Example

The following command creates a capability profile with these settings:

- Specifies a capability profile name of "CapabilityProfile1"
- Specifies that the capability profile is based on "pool_1"
- Specifies the usage tag as "Production"
- Not specified to be created in asynchronous mode

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/cp
create -name "CapabilityProfile1" -pool pool_1 -usageTag "Production"
```

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

ID = cp_1
Operation completed successfully.
```

View capability profiles

Displays a list of existing capability profiles and their characteristics.

Format

```
/stor/config/cp [-id <value>] show
```

Object qualifier

Qualifier	Description
-id	Type the ID of the capability profile.

Example

The following command displays a list of existing capability profiles and their characteristics.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/cp show
-detail
```

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

       ID                = cp_1
       Name              = CapabilityProfile1
       Description       =
       VMware UUID       = 550e8400-e29b-41d4-a716-446655440000
       Storage pool      = pool_1
       Service level     = Gold
       Usage tag         = Exchange, OLTP
       Drive type        = ExtremeMultiTier
       RAID level        = Mixed
       FAST Cache        = Off
       FAST VP policy    = Start high then auto-tier, Auto-tier,
Highest available tier, Lowest available tier
       Space efficiency = Thin, Thick
       Health state      = OK (5)
       Health details    = "The component is operating normally. No
action is required."
```

Change capability profiles

Modify an existing capability profile.

Format

```
/stor/config/cp -id <value> set [-async] [-name <value>] [-
descr <value>] [{-addUsageTag <value> | -removeUsageTag
<value>}]
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the capability profile to be modified.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-name`	Type a name for the capability profile. **Note** The name may contain alphanumeric values, a hyphen, an underscore, and a period. It cannot start with hyphen or period, and cannot consist only of digits.
`-descr`	Type a description for the capability profile.
`-addUsageTag`	Comma-separated list of user-specified usage tags to be added to the specified capability profile. Each tag is an alphanumeric string value.
`-removeUsageTag`	Comma-separated list of user-specified usage tags to be removed from the specified capability profile. Each tag is an alphanumeric string value.

Example

The following command changes the name of capability profile "cp_1".

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/cp -id cp_1 set -name "CapabilityProfile2"`

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

ID = cp_1
Operation completed successfully.
```

Delete capability profiles

Deletes specified capability profiles.

Format

`/stor/config/cp [-id <value>] delete [-async]`

Object qualifier

Qualifier	Description
`-id`	Type the ID of the capability profile.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.

Example

The following command deletes capability profile cp_1.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/cp -id
cp_1 delete
```

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

Operation completed successfully.
```

Manage I/O limits

An I/O policy allows you to limit throughput and bandwidth, providing for more predictable performance in system workloads, that is, between hosts and applications and storage resources.

The following table lists the attributes for I/O limits:

Table 121 I/O limit attributes

Attribute	Description
`ID`	ID of the I/O limit.
`Name`	Name of the I/O limit.
`Description`	Brief description of the I/O limit.
`Shared`	Whether the I/O limit is shared, that is, whether settings are enforced on the sum of all the storage resources that have this policy or on each individual storage resource. Values are one of the following: • `yes` • `no` (default)
`Paused`	Whether the defined I/O limit policy is paused. Values are one of the following: • `yes` • `no`
`Type`	Whether the I/O limit is absolute or density based. Values are one of the following: • `absolute` (default) • `density`
`Maximum IOPS`	Maximum I/O operations per second for an absolute limit policy.

Table 121 I/O limit attributes (continued)

Attribute	Description
`Maximum KBPS`	Maximum KB per second for an absolute limit policy.
`Maximum IOPS per GB`	Maximum IOPS per GB of size for the attached object. This is applicable only when the policy type is density based. The effective limit is the product of the maximum IOPS and the size in GB of the attached object.
`Maximum KBPS per GB`	Maximum KBPS per GB of size for the attached object. This is applicable only when the policy type is density based. The effective limit is the product of the maximum KBPS and the size in GB of the attached object.
`Burst rate`	Amount of traffic over the base I/O limit that can occur during the burst time, expressed as a percentage of the base limit. Burst time and burst frequency must also be specified. Value is 1-100.
`Burst time`	Number of minutes during which traffic may exceed the base limit. Burst rate and burst frequency must also be specified. Use the following format: <*value*><*qualifier*> where: • *value* ■ `minutes` — Number of minutes within the range 1 - 60. • *qualifier* ■ `m` — Indicates minutes. **Note** This setting is not a hard limit and is used only to calculate the extra I/O operations allocated for bursting. The actual burst time depends on I/O activity and may be longer than defined when activity is lower than the allowed burst rate.
`Burst frequency`	Number of hours between the beginning of one burst and the following burst. Burst rate and burst time must also be specified. Use the following format: <*value*><*qualifier*> where: • *value* ■ `hours` — Number of hours within the range 1 - 24. • *qualifier* ■ `h` — Indicates hours. **Note** When a burst policy setting is applied initially or changed, the burst frequency interval begins and the storage that is associated with the policy will burst immediately, regardless of when the last burst occurred.
`Effective IOPS limit`	This is a read-only value that only applies to a shared policy. It is the total effective IOPS for all of the attached objects combined.

Table 121 I/O limit attributes (continued)

Attribute	Description
`Effective KBPS limit`	This is a read-only value that only applies to a shared policy. It is the total effective KBPS for all of the attached objects combined.

Create an I/O limit policy

Create an I/O limit policy that can be applied to a storage resource.

Format

```
/stor/config/iolimit create [-async] -name <value> [-descr
<value>] [-shared {yes | no}] [-type {absolute | density}] [-
maxIOPS <value>] [-maxKBPS <value>] [-maxIOPSDensity <value>]
[-maxKBPSDensity <value>] [-burstRate <value> -burstTime
<value> -burstFrequency <value>]
```

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-name`	Type the name of the I/O limit.
`-descr`	Type a brief description of the I/O limit.
`-shared`	Specify whether the I/O limit is shared. Values are one of the following: - `yes` - `no` (default)
`-type`	Specify whether an absolute or density-based policy will be created. Values are one of the following: - `absolute` (default) - `density`
`-maxIOPS`	Specify the maximum IOPS. Cannot be specified when `-type` is `density`.
`-maxKBPS`	Specify the maximum KBPS. Cannot be specified when `-type` is `density`.
`-maxIOPSDensity`	Specify the maximum IOPS per GB size of the attached object. Cannot be specified when `-type` is `absolute`.
`-maxKBPSDensity`	Specify the maximum KBPS per GB size of the attached object. Cannot be specified when `-type` is `absolute`.
`-burstRate`	Specify the burst rate as a percentage over the base limit. Requires the use of `-burstTime` and `-burstFrequency`. Value is 1 - 100.
`-burstTime`	Specify the time interval during which the burst rate is in effect, in minutes. Requires the use of `-burstRate` and `–burstFrequency`. Use the following format:

Qualifier	Description
	*<value>*m, where: • *<value>*—Number of minutes within the range 1 - 60. • m—Qualifier to identify minutes.
-burstFrequency	Specify how often bursting is allowed in hours. Requires the use of -burstRate and -burstTime. Use the following format: *<value>*h, where: • *<value>*—Number of hours within the range 1 - 24. • h—Qualifier to identify hours.

Example 1

The following command creates an I/O limit policy with these settings:

- Name is finance.
- Description is “for finance department.”
- Shared.
- Type is absolute.
- Maximum IOPS of 500.
- Maximum KBPS of 1000.

The I/O limit policy receives the ID IOL_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/iolimit
create -name "finance" -descr "for finance department" -shared yes -
type absolute -maxIOPS 500 -maxKBPS 1000
```

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

ID = IOL_1
Operation completed successfully.
```

Example 2

The following command creates an I/O limit policy with these settings:

- Name is engineering.
- Description is “for engineering department.”
- Unshared.
- Type is density based.
- Maximum IOPS per GB of 600.
- Maximum KBPS per GB of 2000.
- Burst rate of 30 percent.
- Burst time of five minutes.
- Burst frequency of two hours.

The I/O limit policy receives the ID IOL_2:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/iolimit
create -name "engineering" -descr "for engineering department" -shared
```

```
yes -type density -maxIOPSDensity 600 -maxKBPSDensity 2000 -burstRate
30 -burstTime 5m -burstFrequency 2h
```

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

ID = IOL_2
Operation completed successfully.
```

Example 3

The following command failed because `-type` was set to `absolute`, but options only applicable to a `-type` of `density` were specified.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/iolimit
create -name "HR2" -type absolute -maxIOPSDensity 2000 -maxKBPSDensity
3000
```

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

Operation failed. Error code: 0x900912a
Mismatch between policy type and limit values. Absolute policy
requires Maximum IOPS and/or Maximum KBPS while Density-based
policy requires Maximum IOPS per GB and/or Maximum KBPS per GB.
(Error Code:0x900912a)
```

Example 4

The following command failed because `-type` was set to `density`, but options only applicable to a `-type` of `absolute` were specified.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/iolimit
create -name "HR3" -type density -maxIOPS 2000 -maxKBPS 3000
```

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

Operation failed. Error code: 0x900912a
Mismatch between policy type and limit values. Absolute policy
requires Maximum IOPS and/or Maximum KBPS while Density-based
policy requires Maximum IOPS per GB and/or Maximum KBPS per GB.
(Error Code:0x900912a)
```

Delete an I/O limit policy

Delete an I/O limit policy.

Format

`/stor/config/iolimit -id <value> delete [-async] [-force]`

Object qualifier

Qualifier	Description
`-id`	Type the name of the I/O limit policy.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-force`	Specify whether an I/O limit policy can be deleted when it is still being used by storage resources or snapshots. If not specified, an error is given. Otherwise the I/O limit policy is removed from all storage resources and/or snapshots before it gets deleted.

Example

The following command deletes I/O limit policy IOL_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/iolimit
-id IOL_1 delete
```

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

Operation completed successfully.
```

Change an I/O limit policy

Change the settings of an existing I/O limit policy.

Format

```
/stor/config/iolimit -id <value> set [-async] [-name <value>]
[-descr <value>] [-paused {yes | no}] [-type {absolute |
density}] [{-maxIOPS <value> | -noMaxIOPS}] [{-maxKBPS <value>
| -noMaxKBPS}] [{-maxIOPSDensity <value> | -noMaxIOPSDensity}]
[{-maxKBPSDensity <value> | -noMaxKBPSDensity}] [{-noBurst | [-
burstRate <value> -burstTime <value> -burstFrequency <value>]}]
```

Object qualifier

Qualifier	Description
`-id`	Type the name of the I/O limit policy to change.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-name`	Type the name of the I/O limit.
`-descr`	Type a brief description of the I/O limit.
`-paused`	Indicates whether the defined I/O limit policy is paused or resumed. Values are one of the following: • `yes` • `no` (default)

Qualifier	Description
-type	Specify whether and absolute or density-based policy will be created. Values are one of the following: • absolute (default) • density
-maxIOPS	Specify the maximum IOPS.
-maxKBPS	Specify the maximum KBPS.
-noMaxIOPS	Specify to clear the -maxIOPS setting.
-noMaxKBPS	Specify to clear the -maxKBPS setting.
-maxIOPSDensity	Specify the maximum IOPS per GB size of the attached object.
-maxKBPSDensity	Specify the maximum KBPS per GB size of the attached object.
-nomaxIOPSDensity	Specify to clear the -maxIOPSDensity setting.
-nomaxKBPSDensity	Specify to clear the -maxKBPSDensity setting.
-noBurst	Specify to disable bursting for current I/O limit policy and clear the values for -burstRate, -burstTime, and -burstFrequency.
-burstRate	Specify the burst rate as a percentage over the base limit. Requires the use of -burstTime and -burstFrequency. Value is 1 - 100.
-burstTime	Specify the time interval during which the burst rate is in effect in minutes. Requires the use of -burstRate and -burstFrequency. Use the following format: *<value>*m, where: • *<value>*—Number of minutes within the range 1 - 60. • m—Qualifier to identify minutes.
-burstFrequency	Specify how often bursting is allowed in hours. Requires the use of -burstRate and -burstTime. Use the following format: *<value>*h, where: • *<value>*—Number of hours within the range 1 - 24. • h—Qualifier to identify hours.

Example 1

The following command updates I/O limit policy IOL_1 with these settings:

- Name is engineering.
- Maximum IOPS to 1000.
- Clears the maximum KBPS setting.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/iolimit
-id IOL_1 set -name "engineering" -maxIOPS 1000 -noKBPS
```

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

Operation completed successfully.
```

Example 2

The following command pauses I/O limit policy IOL_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/iolimit
-id IOL_1 set -paused yes
```

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

Operation completed successfully.
```

View I/O limit policies

Display the settings for the specified I/O limit policy or for all existing I/O limit policies.

Format

`/stor/config/iolimit [-id <value>] show`

Object qualifier

Qualifier	Description
`-id`	Type the name of the I/O limit policy to display.

Example

The following command displays details about all I/O limit policies on the system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/iolimit
show -detail
```

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

1:     ID                          = IOL_1
       Name                        = Finance
       Description                 = for finance department
       Shared                      = yes
       Paused                      = yes
       Type                        = absolute
       Maximum IOPS                = 500
       Maximum KBPS                = 1000
       Maximum IOPS per GB         =
       Maximum KBPS per GB         =
       Burst rate                  =
       Burst time                  =
       Burst frequency             =
       Effective IOPS limit        = 500
       Effective KBPS limit        = 1000
```

```
2:     ID                            = IOL_2
       Name                          = Engineering
       Description                   = for engineering department
       Shared                        = no
       Paused                        = no
       Type                          = density
       Maximum IOPS                  =
       Maximum KBPS                  =
       Maximum IOPS per GB           = 600
       Maximum KBPS per GB           = 2000
       Burst rate                    = 30%
       Burst time                    = 5m
       Burst frequency               = 2h
       Effective IOPS limit          = 1800
       Effective KBPS limit          = 6000
```

Note

The object attached to IOL_2 in this example has 3 GB of storage.

Manage I/O limit configuration

An I/O policy allows you to limit throughput and bandwidth, providing for more predictable performance in system workloads, that is, between hosts and applications and storage resources.

An I/O limit policy can be applied to an individual LUN or to a group of LUNs. Only one I/O limit policy can be applied to an individual LUN or a LUN that is a member of a consistency group.

The following table lists the attributes for I/O limit configurations:

Table 122 I/O limit configuration attributes

Attribute	Description
`IO limits paused`	Whether the defined I/O limit policies defined on the system are enforced.
`Maximum controllable storage objects`	Maximum number of storage objects that can have I/O limits enforced; this includes both storage resources and attached snapshots.
`Actively controlled storage objects`	Number of storage objects that currently have I/O limits enforced; this includes both storage resources and attached snapshots.

View I/O limit configuration setting

Display the settings for the existing I/O limit configuration setting.

Format

```
/stor/config/iolimit/config show
```

Example

The following command displays the I/O limits defined on the system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/
iolimit/config show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
1:     IO limits paused                        = yes
       Max controllable storage objects        = 512
       Actively controlled storage objects     = 200
```

Enforce use of I/O limit configuration setting

Enforce the use of the existing I/O limit configuration setting across the system.

Note

Enforcement of host I/O limits is controlled globally across your system. You cannot disable or enable the use of a particular policy.

Format

```
/stor/config/iolimit/config set -paused {yes|no}
```

Action qualifier

Qualifier	Description
`-paused`	Specify whether the I/O limit policies defined on the system are enforced. Value is yes or no.

Example

The following command enforces the use of I/O limits on the system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/
iolimit/config set -paused no
```

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

Operation completed successfully.
```

CHAPTER 7

Protect Data

This chapter contains 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 106 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 for recovering from disasters or the loss of physical equipment.

The following table lists the attributes for snapshots:

Table 123 Snapshot attributes

Attribute	Description
`ID`	ID of the snapshot.
`Name`	Name of the snapshot.
`State`	State of the snapshot. Valid values are: • `initializing` • `ready` • `faulted` • `offline` • `destroying`
`Attached`	Indicates whether the snapshot is attached to a host. **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.
`Attach details`	Comma-separated list of export paths or WWNs for attached snapshots.

Table 123 Snapshot attributes (continued)

Attribute	Description
`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.
`Last refresh time`	Indicates the last time that the snapshot was refreshed.
`Created by`	Name of the user, protection schedule, or backup process that created the snapshot. Valid values are: • 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. Valid values are: • `yes` • `no`
`Allow auto-delete`	Indicates whether or not the system can automatically delete the snapshot. Valid values are: • `yes` • `no` Default value is `yes`.
`Size`	Pool capacity consumed by the snapshot.

Table 123 Snapshot attributes (continued)

Attribute	Description
	Note This field is blank for snapshots of consistency groups and VMware block applications.
`Access`	Indicates whether a file system snapshot is a read-only checkpoint, or read/write for user access.
`IO limit`	Comma-separated IO limit policy IDs for the attached snapshots of block-based storage resources. Members of a snapshot group can have different IO limit policy IDs.
`Effective maximum IOPS`	Dependant on the policy type. For a density-based policy, this value is the product of the maximum IOPS and the size of the attached snapshot. This is a read-only attribute.
`Effective maximum KBPS`	Dependant on the policy type. For a density-based policy, this value is the product of the maximum KBPS and the size of the attached snapshot. This is a read-only attribute.
`Read/write hosts`	Comma-separated list of identifiers of hosts allowed writing data. Applies only if the snapshot is attached to a dynamic snapshot mount point.
`Read-only hosts`	Comma-separated list of identifiers of hosts allowed reading data. Applies only if the snapshot is attached to a dynamic snapshot mount point.
`Replicated`	Indicates whether the snapshot is asynchronously replicated. Valid values: • `no`—Not marked for replication • `pending`—Marked for replication, but waiting synchronization • `yes`—Successfully replicated to destination • `failed to replicate, check System Alerts for details`—Failed to replicate
`Sync replicated`	Indicates whether the snapshot participates in a synchronous replication session. Valid values: • `no`—Either the snapshot was created on the destination site and will not be replicated on the source, or the snapshot was created before a synchronous replication session was set up. • `yes`—Successfully replicated. • `failed to replicate`—Snapshot was created on the source site while a replication session was in a fractured state. The snapshot was not replicated to the destination site.
`Remote expiration time`	Time when the snapshot will be removed on the destination.
`Remote allow auto-delete`	Indicates whether this snapshot participates in auto-delete on the destination. Valid values are:

Table 123 Snapshot attributes (continued)

Attribute	Description
	• `yes` • `no` Default value is `no`.

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 400 explains how to view the current protection storage size for file systems. View LUNs on page 450 explains how to view the current protection size for LUNs.

Format

```
/prot/snap create [-async] [-name <value>] [-descr <value>] [{-keepFor <value> | -allowAutoDelete {yes | no}}] [-access {ckpt | share}] [-replicate [{-keepSameAsSource | -keepRemotelyFor <value> | -allowRemoteAutoDelete {yes | no}}]]
```

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 400 explains how to view the settings for file systems. View consistency groups on page 462 explains how to view the settings for iSCSI storage resources
`-keepFor`	Specify the amount of time to retain a snapshot before it expires. The interval can be defined in days or hours. The system deletes expired snapshots automatically. Use the following format: *`<value><qualifier>`* where: • `value` — Type the number of hours or days:

Qualifier	Description
	▪ For hours, the range is 1–8760. ▪ For days, the range is 1–365. • `qualifier` — Type the value qualifier. Value is one of the following: ▪ `h` – Indicates hours. ▪ `d` – Indicates 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 108 provides details about schedule rules.
`-allowAutoDelete`	Specify whether the system can automatically delete the snapshot or snapshot set. Valid values are: • `yes` (default) • `no`
`-access`	Specify whether the snapshot is a read-only checkpoint, or read/write for CIFS (SMB) shares or NFS exports. Valid values are: • `ckpt` (default) • `share`
`-replicateSnap`	Specify whether to mark this snapshot for replication. Valid values: • `yes` • `no` (default)
`-keepSameAsSource`	Indicates whether to use the same retention policy (expiration time and auto-delete) of the source for the destination. This is a one-time copy of the source snapshot retention policy and the remote retention policy does not update if the source retention policy is changed. No values are allowed.
`-keepRemotelyFor`	Specifies the retention time after which the snapshot is deleted on the destination. The interval can be defined in days or hours. The format of the value is as follows: *`<value><qualifier>`* where: • *value* - - An integer value. If the *qualifier* is `h` (hours), the valid range is from 1 to 61194. If the *qualifier* is `d` (days), the valid range is from 1 to 2549.

Qualifier	Description
	• *qualifier* - A value qualifier. The valid values are `h` (hours) and `d` (days).
`-allowRemoteAutoDelete`	Indicates whether auto delete is allowed on the replicated copy of this snapshot or snapshot set. Valid values are: • `yes` • `no`

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 23 explains how to change the output format.

Format

/prot/snap [{-id *<value>* | -name *<value>*} [-members] | -source *<value>*}] show

Object qualifier

Qualifier	Description
`-id`	Identifies the ID of a snapshot.
`-name`	Identifies the name of the snapshot.
`-members`	Flag indicating that only member snapshots will be shown.

Qualifier	Description
	Note This is applicable to snapshots of Consistency groups and VMware VMFS storage resources only.
`-source`	Identifies 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 -detail`

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

1:     ID                        = 171798691881
       Name                      = FS_Snapshot1
       State                     = Ready
       Attached                  = no
       Resource                  = res_1
       Resource Type             = File system
       Source                    = res_1
       Source Type               = File system
       Members                   =
       Attach details            =
       Source Snapshot           =
       Description               =
       Creation time             = 2016-06-27 17:02:07
       Expiration time           = Never
       Last writable time        = Never
       Last refresh time         = Never
       Created by                = admin
       Modified                  = no
       Allow auto-delete         = yes
       Size                      = 3221225472 (3.0G)
       Access                    = Protocol
       IO limit                  =
       Effective maximum IOPS    =
       Effective maximum KBPS    =
       Replicated                = pending
       Sync replicated           = no
       Remote expiration time    = Never
       Remote allow auto-delete  = yes
       Read/write hosts          =
       Read-only hosts           =
```

Attach snapshots to hosts

For snapshots of storage resources, attach a snapshot to make it available to hosts.

Note

If the default attach type is used, before a host can access an attached snapshot, it must have snapshot permissions to the appropriate storage resource. Manage LUNs on page 442 explains how to configure host access permissions for LUN storage resources.

Format

```
/prot/snap {-id <value> | -name <value>} attach [-async] [-copyName <value>] [-type {default | dynamic [-roHosts <value>] [-rwHosts <value>][-force {yes | no}]}]
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the snapshot to attach.
`-name`	Type the name of the snapshot to attach.

Action qualifiers

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-copyName`	Specify 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.
`-type`	Attachment type. Valid values are (case insensitive): • `default` (default)—Allows promoting only one snapshot of the parent storage resource at a time. • `dynamic`—Allows promoting several snapshots of the same parent storage resource simultaneously.
`-roHosts`	Specify the comma-separated list of hosts that have read-only access to the snapshot.
`-rwHosts`	Specify the comma-separated list of hosts that have read/write access to the snapshot.
`-force`	Specify that read-write access for the snapshot can be configured, even though the object has independent thin clones. Valid values are: • `yes` • `no` (default)

Example

The following command attaches snapshot SNAP_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap -id
SNAP_1 attach -type dynamic -roHosts Host_1,Host_2 -rwHosts
Host_3,Host_4
```

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

```
Operation completed successfully.
```

Refresh snapshots

Note

The refresh snapshots command is only valid for block snapshots.

Format

```
/prot/snap {-id <value> | -name <value>} refresh [-async] [-copyName <value>]
```

Object qualifier

Qualifier	Description
`-id`	ID of the snapshot to refresh.
`-name`	Name of the snapshot to refresh.

Action qualifiers

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-copyName`	Specify the name of the copy the system creates before the refresh operation. If the name specified is blank (" "), a copy will be created with a date/time stamp name. **Note** If this switch is not specified, no copy is created.

Example

The following command refreshes a snapshot:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap -id 38654705680 refresh –copyName copy1
```

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

ID = 38654705680
Operation completed successfully
```

Replicate snapshots

Note

Use to replicate snapshots after they have been created.

Format

```
/prot/snap {-id <value> | -name <value>} replicate {-
keepSameAsSource | -keepRemotelyFor <value> | -
allowRemoteAutoDelete {yes | no}}
```

Object qualifier

Qualifier	Description
`-id`	Identifies the snapshot.
`-name`	Identifies the snapshot by its name.

Action qualifier

Qualifier	Description
`-keepSameAsSource`	Indicates whether or not to use the same retention policy (expiration time and auto-delete) of the source for the destination. This is a one-time copy of the source snapshot retention policy and the remote retention policy does not update if the source retention policy is changed.
`-keepRemotelyFor`	Specifies the retention period after which the snapshot is deleted on the destination. The interval can be defined in days or hours. The format of the value is the following: *`<value><qualifier>`* where: • `value`—Type the number of hours or days: ▪ For hours, the range is 1–61194. ▪ For days, the range is 1–2549. • `qualifier`—Type the value qualifier. Value is one of the following: ▪ `h`—Indicates hours. ▪ `d`—Indicates days.
`-allowRemoteAutoDelete`	Indicates whether auto delete is allowed on the replicated copy of this Snapshot or Snapshot Set. Valid values are: • `yes` • `no`

Example

The following command replicates a snapshot:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap –id 38654705680 replicate -keepRemotelyFor 1d`

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

```
HTTPS connection

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 442 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.
`-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.

When you restore a storage resource to a snapshot, before the restoration begins, the system will automatically create a snapshot of the storage resource's current state. This ensures that there is no unintentional data loss because of the restore operation. You can use this new snapshot later to restore the storage resource back to its previous state, if necessary.

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 attached, you must first detach 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, 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] [-
overrideLock] [-force]
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the snapshot to delete.
`-name`	Type the name of the snapshot.

Action qualifiers

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-overrideLock`	Override the restriction preventing the deletion of a snapshot that is locked by an application. Attempting to delete a locked snapshot without this option specified will return an error message containing the details of the application that has the snapshot locked. **Note** Do not use this option if applications are currently referencing the snap, to avoid a performance impact on these applications. This option will not bypass all restrictions, only the lock that certain applications may have on the snapshot.
`-force`	Unconditionally removes the snapshot on the destination site, even if it is marked as replicated by the synchronous replication session. **Note** This option is applicable for synchronous destination site snapshots only.

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}}] [-roHosts <value> -rwHosts <value>] [-force]
```

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`	Specify the amount of time to retain a snapshot before it expires. The interval can be defined in days or hours. 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 1–8760. ▪ For days, the range is 1–365. • `<qualifier>`—Type the value qualifier. Value is one of the following: ▪ `h`—Indicates hours. ▪ `d`—Indicates 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 108 provides details about schedule rules.
`-allowAutoDelete`	Specify whether the system can automatically delete the snapshot or snapshot set. Valid values are: • `yes`

Qualifier	Description
	• `no`
`-roHosts`	Specify a comma-separated list of hosts that will have read-only access to the snapshot. This option applies only if the snapshot is attached to a dynamic snapshot mount point.
`-rwHosts`	Specify a comma-separated list of hosts that will have read/write access to the snapshot. This option applies only if the snapshot is attached to a dynamic snapshot mount point.
`-force`	Unconditionally modifies the snapshot on the destination site, even if it is marked as replicated by the synchronous replication session. **Note** This option is applicable for synchronous destination site snapshots only.

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 124 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 532.)
`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

Table 124 Snapshot NFS share attributes (continued)

Attribute	Description
	• `root` — Root access • `na` — No access
`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.
`Role`	Role of the snapshot NFS share. Valid values are: • `backup` – Indicates that the snapshot share is operating in a backup role. Applies to snapshot shares created for the purposes of backup and disaster/recovery on a NAS server operating in a replication destination mode. **Note** When a NAS server fails over, and becomes the source system in a replication, the role of snapshot shares on the NAS server still reflect the backup role. • `production` – Indicates that the snapshot share is operating in a production role. On NAS servers that are not acting as a replication destination, all snapshot shares operate in a production mode.
`Minimum security`	The minimal security option that must be provided by a client for the NFS mount operation. Valid values are (from least secure to most secure): • `sys` – Also known as AUTH_SYS security. This indicates there is no server-side authentication. When secure NFS is not configured on a NAS server, this is the default value. • `krb5` – Kerberos v5 authentication. This is the default value when secure NFS is configured on the NAS server. • `krb5i` – Kerberos v5 authentication and integrity. • `krb5p` – Kerberos v5 authentication and integrity, with encryption enabled.

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>] [-secEnforced {sys | krb5 | krb5i | krb5p}]
```

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. Valid values are: • `ro` — Read-only access • `rw` — Read/Write access • `root` — Root access • `na` — No access
`-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

Qualifier	Description
	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.
`-secEnforced`	Specifies the minimal security option that must be provided by a client for the NFS mount operation. Valid values are (from least secure to most secure): • `sys` – Also known as AUTH_SYS security. This indicates there is no server-side authentication. When secure NFS is not configured on a NAS server, this is the default value. • `krb5` – Kerberos v5 authentication. This is the default value when secure NFS is configured on the NAS server. • `krb5i` – Kerberos v5 authentication and integrity. • `krb5p` – Kerberos v5 authentication and integrity, with encryption enabled.

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> | -name <value> | -snap <value> | -snapName <value>}] show`

Object qualifier

Qualifier	Description
`-id`	ID of the NFS share.
`-name`	Name of the NFS share.
`-snap`	ID of the parent snapshot. The list of shares associated with the identified snapshot will be displayed.
`-snapName`	Name of 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
      Role                = production
      Minimum security   = krb5
```

Set snapshot NFS share

Modifies an existing snapshot NFS share.

Format

```
/prot/snap/nfs {-id <value> | -name <value>} set [-async] [-
descr <value>] [-defAccess {ro | rw | root | na}] [-roHosts
<value>] [-rwHosts <value>] [-rootHosts <value>] [-naHosts
<value>] [-minSecurity {sys | krb5 | krb5i | krb5p}]
```

Object qualifier

Qualifier	Description
`-id`	ID of the snapshot NFS share.
`-name`	Name of the snapshot NFS share.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.
`-descr`	Type the description of the share.
`-defAccess`	Specifies the new user description of the share. Valid values are: • `ro`—Read-only access • `rw`—Read/write access • `root`—Root access • `na`—No access
`-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.
`-minSecurity`	Specifies the minimal security option that must be provided by a client for the NFS mount operation. Valid values are (from least secure to most secure): • `sys`—Also known as AUTH_SYS security. This indicates there is no server-side authentication. When secure NFS is not configured on a NAS server, this is the default value. • `krb5`—Kerberos v5 authentication. This is the default value when secure NFS is configured on the NAS server. • `krb5i`—Kerberos v5 authentication and integrity. • `krb5p`—Kerberos v5 authentication and integrity, with encryption enabled.

Example

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap/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 share, you can no longer recover data from it or restore a storage resource to it.

Format

`/prot/snap/nfs {-id <value> | -name <value>} delete [-async]`

Object qualifier

Qualifier	Description
`-id`	Type the ID of the snapshot to delete.
`-name`	Type the name 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 (SMB) shares.

Table 125 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 532.)
`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.
`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

Table 125 Snapshot CIFS share attributes (continued)

Attribute	Description
	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 (SMB) 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 on which to mount the shared file system.
`-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.

Qualifier	Description
`-enableABE`	Specify if Access-based Enumeration is enabled. Valid values are: • `yes` • `no` (default)
`-enableBranchCache`	Specify if BranchCache is enabled. Valid values are: • `yes` • `no` (default)
`-offlineAvailability`	Specify the type of offline availability. Valid values are: • `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 (SMB) shares.

Format

```
/prot/snap/cifs [{-id <value> | -name <value> | -snap <value> |
-snapName <value>}] show
```

Object qualifier

Qualifier	Description
-id	ID of the CIFS share.
-name	Name of the CIFS share.
-snap	ID of the parent snapshot. The list of shares associated with the identified snapshot will be displayed.
-snapName	Name of 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 CIFS (SMB) share.

Format

```
/prot/snap/cifs {-id <value> | -name <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	ID of the snapshot CIFS share.
-name	Name of the snapshot CIFS share.

Action qualifier

Qualifier	Description
-async	Run the operation in asynchronous mode.

Qualifier	Description
-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 are: • yes • no
-enableBranchCache	Specify if BranchCache is enabled. Valid values are: • yes • no
-offlineAvailability	Specify the type of offline availability. Valid values are: • none—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 /prot/snap/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 (SMB) share.

Note

Once you delete a snapshot share, you can no longer recover data from it or restore a storage resource to it.

Format

```
/prot/snap/cifs {-id <value> | -name <value>} delete [-async]
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the snapshot to delete.
`-name`	Type the name of the snapshot to delete.

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
smb_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.

It is important to note that when replicating from a Unity system running a later OE version (for example, OE 4.1.x) to a Unity system running an older version (for example, OE 4.0.x), you cannot have new OE version features enabled on the source.

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 126 Replication session attributes

Attribute	Description
`ID`	ID of the session.
`Name`	Name of the replication session.
`Session type`	Storage type of the session. Valid values are: - `lun` - `block` - `file` - `nas server`
`Synchronization type`	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. - `sync`—Data is synchronously replicated with RPO=0. **Note** For asynchronous replication, the potential for data loss increases as the RPO 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. For synchronous replication, the RPO is set to 0 automatically.
`Resource type`	Type of storage resource to which the replication session is applied. Valid values are: - `LUN` - `LUN group` - `File System` - `VMware VMFS` - `VMware NFS` - `NAS Server`
`Sync State`	Additional state of the replication session, specific to the replication mode.

Table 126 Replication session attributes (continued)

Attribute	Description
	- For asynchronous replication, valid values are: ■ idle— No active syncing. ■ manual— User initiated syncing. ■ auto syncing— System initiated syncing. - For synchronous replication, valid values are: ■ unknown—Unknown sync state. ■ out of sync—Destination is out of sync with the source. ■ in sync—Destination is an exact copy of the source. ■ consistent—Destination is a point in time copy of the source. ■ syncing—System initiated syncing. ■ inconsistent—Destination is not a point in time copy of the source.
Health state	Health state of the session. Valid values are: - Unknown—Session health cannot be determined. - OK—Session is operating normally. - Degraded/Warning—An error has caused one or more of the following: ■ Session has been paused. ■ 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 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. ■ Session is syncing. - Minor failure—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. - Critical failure— Session has encountered an error that has halted the session. **Note** If the replication session is in an error state, in addition to resolving the issue (for example, destination pool out of space), try pausing, and then resuming the replication session. If the problem persists, delete and then create the replication session again.
Health details	Additional health information.

Table 126 Replication session attributes (continued)

Attribute	Description
Operational status	Operational status of the session. The operational status code appears in parentheses. • Unknown (0x0) • Non Recoverable Error (0x7) • Lost Communication (0xd) • Failed Over with Sync (0x8400) • Failed Over (0x8401) • Manual Syncing (0x8402) • Paused (0x8403) • Idle (0x8404) • Auto Sync Configured (0x8405) • Destination Extend Failed Not Syncing (0x840B) • Destination Extend In Progress (0x840C) • Active (0x840D) • Lost Sync Communication (0x840E) • Syncing (0x8411)
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 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 failed over state, the destination object is read/write. When communication is reestablished between the source and destination, the source is shown as Restricted Replication Access = Yes. To resume operations on the source site, the replication session needs to be failed back. • Switched over—The replication session has switched over to the source site. In a switched over state, the source object is read/write. When communication is reestablished between the source and destination, the destination is shown as Restricted Replication Access = Yes. To resume operations on the destination site, the replication session needs to be failed over.

Table 126 Replication session attributes (continued)

Attribute	Description
`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 failed over state, the destination object is read/write. When communication is reestablished between the source and destination, the source is shown as Restricted Replication Access = Yes. To resume operations on the source site, the replication session needs to be failed back. - `Switched over`—The replication session has switched over to the source site. In a switched over state, the source object is read/write. When communication is reestablished between the source and destination, the destination is shown as Restricted Replication Access = Yes. To resume operations on the destination site, the replication session needs to be failed over.
`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 (lost IP) between the systems. A change in the network configuration on either side could also interrupt communication. - `Lost Sync Communication`—Fiber Channel communication with the synchronous replication remote system has been lost. It is likely that the Fiber Channel connection has encountered issues.
`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.

Table 126 Replication session attributes (continued)

Attribute	Description
	- `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.
`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.
`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 resource`	ID of the storage resource on which the data is replicated.
`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.
`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. **Note** For synchronous replication, the percentage is reported when the replication is in the Syncing state.
`Sync transfer rate`	Synchronization transfer rate when the session is in the syncing state. For multi-LUN applications there is a comma-separated list of values.

Table 126 Replication session attributes (continued)

Attribute	Description
	Note This attribute is valid for asynchronous replications only.
`Sync transfer size remaining`	Remaining size to be transferred during synchronization. For multi-LUN applications there is a comma-separated list of values. **Note** This attribute is valid for asynchronous replications only.
`Previous transfer rate`	Previous average transfer rate for the replication session. **Note** This attribute is valid for asynchronous replications only.
`Average transfer rate`	Average transfer rate for the replication session. **Note** This attribute is valid for asynchronous replications only.
`Element pairs`	For consistency group and VMware VMFS datastore replications, the LUN element pairs within the replication.
`Hourly snapshot keep for`	Amount of time to keep replicated hourly snapshots on the destination. Output can be: • Blank when scheduled snapshots are not replicated. • <*value*><*qualifier*>—When a retention duration is specified, where: ■ *value*—An integer value. If the *qualifier* is `h` (hours), the valid range is from 1 to 8760. If the *qualifier* is `d` (days), the valid range is from 1 to 365. ■ *qualifier*—A value qualifier. The valid values are: – `h` (hours) – `d` (days) • `Forever`—When `-keepFor` value is not specified and allow auto-delete is requested • `Same as source`—Keep the destination retention policy the same as the source retention policy **Note** This attribute is valid for asynchronous replications only.
`Hourly snapshot allow auto-delete`	Whether or not the destination pool's auto-delete policy allows replicated hourly snapshots on the destination to be deleted. Output can be:

Table 126 Replication session attributes (continued)

Attribute	Description
	• Blank when scheduled snapshots are not replicated. • `Same as source`—Keep the destination retention policy the same as the source retention policy • `yes`—When `-allowAutoDelete` is set • `no`—When `-keepFor` is set **Note** This attribute is valid for asynchronous replications only.
`Daily snapshot keep for`	Amount of time to keep replicated daily snapshots on the destination. Output can be: • Blank when scheduled snapshots are not replicated. • *value*—An integer value. If the *qualifier* is `h` (hours), the valid range is from 1 to 8760. If the *qualifier* is `d` (days), the valid range is from 1 to 365. • *qualifier*—A value qualifier. The valid values are: ■ `h` (hours) ■ `d` (days) • `Same as source`—Keep the destination retention policy the same as the source retention policy **Note** This attribute is valid for asynchronous replications only.
`Daily snapshot allow auto-delete`	Whether or not the destination pool's auto-delete policy allows the replicated daily snapshots on the destination to be deleted. Output can be: • Blank when scheduled snapshots are not replicated. • `Same as source`—Keep the destination retention policy the same as the source retention policy • `yes`—When `-allowAutoDelete` is set • `no`—When `-keepFor` is set **Note** This attribute is valid for asynchronous replications only.

Create replication sessions

Create a replication session.

NOTICE

Snapshots that have been created and attached as well as read/write (share) snapshots (as opposed to read-only checkpoint snapshots) are not eligible for replication. Only unattached (read-only) snapshots are eligible for replication. For asynchronous replication, you can replicate existing snapshots and snapshots created from snapshot schedules. For synchronous file replication, you cannot replicate existing snapshots or snapshots created from snapshot schedules. You can only replicate those snapshots and snapshots created from snapshot schedules after you have established the synchronous replication session and it is Active.

Note

On a NAS server protected by replication, you must create a replication session for each file system on it. Otherwise, file system related configurations like shares and exports may be lost after a NAS server replication session failover.

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.
- For asynchronous replication in a coexisting asynchronous and synchronous replication with one source resource topology, create the asynchronous replication destination NAS server with both the `-replDest` and the `-backupOnly` attributes set to **`yes`**. These attributes must be set to **`yes`** on the asynchronous replication destination NAS server when the source NAS server is synchronous replicated; otherwise, the asynchronous replication session cannot be created.

Format

```
/prot/rep/session create [-async] -srcRes <value> [-
srcSPAInterface <value>] [-srcSPBInterface <value>] -dstType
{local | remote -dstSys <value>} -dstRes <value> [-
dstSPAInterface <value>] [-dstSPBInterface <value>] [-name
<value>] [-elementPairs <value>] [-syncType {manual [-
autoInitiate {yes | no}] | auto [-rpo <value>]}[-
replicateHourlySnaps {yes [{-keepSameAsSource | -keepFor
<value> | -allowAutoDelete}] | no}] [-replicateDailySnaps {yes
[{-keepSameAsSource | -keepFor <value> | -allowAutoDelete}] |
no}] [-replicateExistingSnaps]
```

Action qualifiers

Qualifier	Description
`-async`	Run an action in asynchronous mode.
`-srcRes`	Type the ID of the storage resource to use as the source.
`-srcSPAInterface`	Type the ID of the interface on the SPA of the source system for the replication.

Qualifier	Description
	Note This qualifier is used for asynchronous 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 asynchronous replications on remote systems only. If the qualifier is not specified, the system identifies the interface automatically.
`-dstType`	Specify the type of destination. 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.
`-dstSys`	For remote replication, type the ID of the destination system. View settings for remote storage systems on page 304 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`

Qualifier	Description
`-dstSPAInterface`	Type the ID of the interface on the SPA of the destination system for the replication. **Note** This qualifier is used for asynchronous 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 asynchronous 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** This qualifier is used for asynchronous replications only. 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. Valid values are: • `yes` • `no` **Note** This qualifier is used for asynchronous replications only.

Qualifier	Description
-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. For synchronous replication, specify the value 0. Once set, the value cannot be reset from zero to non-zero or from non-zero to zero.
-replicateHourlySnaps	Specify whether or not to mark hourly scheduled snapshots for replication. Valid values are: • `yes` • `no` **Note** This qualifier is used for asynchronous replications only.
-replicateDailySnaps	Specify whether or not to mark daily scheduled snapshots for replication. Valid values are: • `yes` • `no` **Note** This qualifier is used for asynchronous replications only.
-keepSameAsSource	Indicates whether or not to use the same retention policy (expiration time and auto-delete) of the source for the destination. This option propagates changes made to the source retention policy to the destination retention policy (from that point forward for newly created scheduled snapshots, old snapshots are left as is). No values are allowed. This option is enabled by default if `-keepFor` or `–allowAutoDelete` are not set. **Note** This qualifier is used for asynchronous replications only.
-keepFor	Specifies the retention time after which the snapshot is deleted on the destination. The interval can be defined in days or hours. Use the following format:

Qualifier	Description
	`<value><qualifier>` where: • *value*—An integer value. If the *qualifier* is `h` (hours), the valid range is from 1 to 61194. If the *qualifier* is `d` (days), the valid range is from 1 to 2549. • *qualifier*—A value qualifier. The valid values are: ▪ `h` (hours) ▪ `d` (days) **Note** This qualifier is used for asynchronous replications only.
`-allowAutoDelete`	Specify whether auto delete is allowed on the replicated copy of this snapshot or snapshot set. Valid values: • `yes` • `no` **Note** This qualifier is used for asynchronous replications only.
`-replicateExistingSnaps`	Indicates whether or not to replicate snapshots already existing on the source resource. This is a one-time option available during session creation that will replicate snapshots existing on the source at that moment in time. All eligible snapshots are replicated and have the source retention policy applied for the destination retention policy. For a snapshot to be eligible for this option, it must meet these 3 criteria: • The snapshot is created by either the user or a snapshot schedule. • The snapshot is read-only (file resource snapshot must be a checkpoint snapshot; block resource snapshot must not be attached). • The snapshot is not currently undergoing deletion. **Note** This qualifier is used for asynchronous replications only.

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.

Note

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

Format

/prot/rep/session [{-id *<value>* | -name *<value>* | -res *<value>*}] show

Object qualifiers

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 1

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         = nas server
      Synchronization type = auto
      Resource type        = NAS Server
      Destination type     = remote
```

Example 2

The following command displays all replication sessions on the system and their details:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session show -detail`

```
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                      = nas server
      Synchronization type              = auto
      RPO                               = 
      Resource type                     = LUN
      Sync State                        = idle
      Health state                      = OK (5)
      Health details                    = "This replication session 
is operating normally. No action is required."
      Operational status                = Idle (0x8404)
      Source status                     = OK
      Destination status                = OK
      Network status                    = OK
      Destination type                  = local
      Destination system                = local
      Local role                        = Local
      Source resource                   = sv_1
      Source SP-A interface             = N/A
      Source SP-B interface             = N/A
      Destination resource              = sv_2
      Destination SP-A interface        = N/A
      Destination SP-B interface        = N/A
      Time of last sync                 = N/A
      Sync status                       = 
      Sync transfer rate                = N/A
      Sync transfer size remaining      = 0
      Previous transfer rate            = N/A
      Average transfer rate             = N/A
      Element pairs                     = N/A
      Hourly snapshot keep for          = 3h
      Hourly snapshot allow auto-delete = no
      Daily snapshot keep for           = same as source
      Daily snapshot allow auto-delete  = same as source
```

Change replication session settings

Change the settings for a replication session.

Format

/prot/rep/session {–id *<value>* | -name *<value>*} set [-async] [-newName *<value>*] [-srcSPAInterface *<value>*] [-dstSPAInterface *<value>*] [-srcSPBInterface *<value>*] [-dstSPBInterface *<value>*] [-syncType {manual | auto -rpo *<value>*}] [-replicateHourlySnaps {yes [{-keepSameAsSource | -keepFor *<value>* | -

```
allowAutoDelete}] | no}] [-replicateDailySnaps {yes [{-
keepSameAsSource | -keepFor <value> | -allowAutoDelete}] | no}]
```

Object qualifiers

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
`-async`	Run an action in asynchronous mode.
`-newName`	Type the new name of the replication session.
`-srcSPAInterface`	Type the ID of the interface on the SPA of the source system for the replication. **Note** This qualifier is used for asynchronous 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 asynchronous 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 asynchronous 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 asynchronous 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:

Qualifier	Description
	- 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** This qualifier is used for asynchronous replications only. 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. **Note** For synchronous replication, specify the value 0. The value cannot be reset from zero to non-zero or from non-zero to zero.
-replicateHourlySnaps	Specify whether or not to mark hourly scheduled snapshots for replication. Valid values are: - yes - no **Note** This qualifier is used for asynchronous replications only.
-replicateDailySnaps	Specify whether or not to mark daily scheduled snapshots for replication. Valid values are: - yes - no

Qualifier	Description
	Note This qualifier is used for asynchronous replications only.
`-keepSameAsSource`	Specify whether or not to use the same retention policy (expiration time and auto-delete) of the source for the destination. This option propagates changes made to the source retention policy to the destination retention policy (from that point forward for newly created scheduled snapshots, old snapshots are left as is). No values are allowed. **Note** This qualifier is used for asynchronous replications only.
`-keepFor`	Specify the retention time after which the snapshot is deleted on the destination. The interval can be defined in days or hours. Use the following format: *`<value><qualifier>`* where: • *value*—An integer value. If the *qualifier* is `h` (hours), the valid range is from 1 to 61194. If the *qualifier* is `d` (days), the valid range is from 1 to 2549. • *qualifier*—A value qualifier. The valid values are: ▪ `h` (hours) ▪ `d` (days) **Note** This qualifier is used for asynchronous replications only.
`-allowAutoDelete`	**Note** Only valid when **`-replicateHourlySnaps yes`** or **`-replicateDailySnaps yes`**. Specify whether auto delete is allowed on the replicated copy of this snapshot or snapshot set. Valid values are: • `yes` • `no`

Qualifier	Description
	Note This qualifier is used for asynchronous replications only.

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.
```

Pause replication sessions

Pause a replication session.

Format

`/prot/rep/session {-id <value> | -name <value>} pause [-async]`

Object qualifiers

Qualifier	Description
-id	Type the ID of the replication session to be paused.
-name	Type the name of the replication session to be paused.

Action qualifiers

Qualifier	Description
-async	Run an action in asynchronous mode.

Example

The following command pauses replication session 81604378625_FCNCH097274B3A_0000_81604378627_FCNCH097274B37_0000:

```
uemcli /prot/rep/session -id
81604378625_FCNCH097274B3A_0000_81604378627_FCNCH097274B37_0000 pause
```

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

```
Operation completed successfully.
```

Resume replication sessions

Resumes an existing replication session.

Format

```
/prot/rep/session {-id <value> | -name <value>} resume [-async]
[-forceFullCopy] [-srcSPAInterface <value>] [-dstSPAInterface
<value>] [-srcSPBInterface value>] [-dstSPBInterface <value>]
```

Object qualifiers

Qualifier	Description
`-id`	Type the ID of the replication session to be resumed.
`-name`	Type the name of the replication session to be resumed.

Action qualifiers

Qualifier	Description
`-async`	Run an action in asynchronous mode.
`-forceFullCopy`	Specifies to force a full synchronization during the resume operation.
`-srcSPAInterface`	Type the ID of the interface on the SPA of the source system for the replication. **Note** This qualifier is used for asynchronous 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 asynchronous 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 asynchronous 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 asynchronous replications on remote systems only. If the qualifier is not specified, the system identifies the interface automatically.

Example

The following command resumes replication session 81604378625_FCNCH097274B3A_0000_81604378627_FCNCH097274B37_0000:

```
uemcli /prot/rep/session -id 81604378625_FCNCH097274B3A_0000_81604378627_FCNCH097274B37_0000 resume
```

```
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 [-async]`

Object qualifiers

Qualifier	Description
`-id`	Type the ID of the replication session to synchronize.
`-name`	Type the name of the replication session to synchronize.

Action qualifiers

Qualifier	Description
`-async`	Run an action in asynchronous mode.

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. Deleting the session from the source system automatically removes the destination and source replication sessions. This ensures that you do not have to manually delete the associated storage resources or NAS servers from the destination system.

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. When deleting a file system synchronous replication session, though the session is deleted, if the initial synchronization does not complete, the destination file system will run into an unrecoverable error. In this case, delete the destination file system.

Format

```
/prot/rep/session {-id <value> | -name <value>} delete [-async]
```

Object qualifiers

Qualifier	Description
`-id`	Type the ID of the replication session to delete.
`-name`	Type the name of the replication session to delete.

Action qualifiers

Qualifier	Description
`-async`	Run an action in asynchronous mode.

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 582 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 [-
async] [-sync {yes | no}] [-force]
```

Object qualifiers

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 qualifiers

Qualifier	Description
`-async`	Run an action in asynchronous mode.
`-sync`	For an asynchronous replication session, specifies whether a synchronization needs to be performed before failing over the replication session. For a synchronous replication session, specifies whether to keep synchronization on the reversed direction after failing over the session. Valid values are: • `yes`—For a planned failover. Can only be issued from the source system. Where `-sync` is not specified, this is the default value for a local replication session or session where `role=source`. • `no`—For an unplanned failover. Can only be issued from the destination system. Where `-sync` is not specified, this is the default value for a remote replication session or session where `role=destination`.

Qualifier	Description
	Note If the Network status=OK, the source system is probably OK. The command issued from the destination system without this option will fail. It is recommended to rerun the command using the `yes` option from the source system. However, in that case, the command issued from the destination system using the `no` option is still allowed.
`-force`	Specifies whether to skip a pre-check operation on file systems of a NAS server when a replication failover operation is issued from the source NAS server. No values are allowed.

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 [-async] [-forceFullCopy] [-force]
```

Object qualifiers

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 qualifiers

Qualifier	Description
-async	Run an action in asynchronous mode.
-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. • This qualifier is used for asynchronous replications only.
-force	Before failing back a NAS server synchronous replication session, it is checked whether its associated asynchronous file system replication sessions are all preserved when coexisting. When this qualifier is specified, that check is skipped.

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.
```

Preserve asynchronous replication sessions

Initiates a preserve asynchronous replication sessions operation on a NAS server synchronous replication session. After a NAS server synchronous replication session fails over or fails back with its file system synchronous replication sessions, the asynchronous replication sessions will be switched to the new production site by the preserve asynchronous replication sessions operation.

Format

```
/prot/rep/session {-id <value> | -name <value>} preserveAsync
```

Object qualifiers

Qualifier	Description
-id	Identifies the NAS server synchronous replication session.
-name	Identifies the NAS server synchronous replication session by name.

Example

The following command preserves asynchronous replication sessions for 81604378625_FCNCH097274B3A_0000_81604378627_FCNCH097274B37_0000:

```
uemcli /prot/rep/session -id
81604378625_FCNCH097274B3A_0000_81604378627_FCNCH097274B37_0000
preserveAsync
```

```
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 virtual 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 291.
- 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 127 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: • `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: • `ascii` - Secret in the ASCII format. • `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 Data at Rest Encryption (physical deployments only)

Note

This feature may not be available in your implementation.

Table 128 Data at Rest Encryption attributes

Attribute	Description
`Encryption mode`	Encryption mode. Valid values are: - `Unencrypted` - `Controller Based Encryption`
`Encryption status`	Status of the encryption process. Valid values are: - `Not encrypting` - `In progress` - `Encrypted` - `Scrubbing` **Note** This attribute is not applicable, and is blank, when the license for the feature is not installed.
`Percent encrypted`	Percent of user data encrypted.
`Backup keystore status`	Status of the keystore backup. Valid values are: - `No operation required` - `Keystore is inaccessible` - `Backup keystore operation required` - `Backup keystore operation in progress` - `Backup keystore operation complete` The keystore must be backed up, using the uemcli –`download` command, and stored off the storage system. **Note** This attribute is not applicable, and is blank, when the license for the feature is not installed.
`KMIP status`	Status of KMIP support. Valid values are: - `Enabled`—KMIP feature is enabled. - `Disabled`—KMIP feature is disabled. - `Unsupported`—KMIP feature is not supported. - `Unknown`—KMIP feature status cannot be determined. **Note** Once enabled, allows the storage system to interact with external key management servers that are KMIP compliant for key management associated with Data at Rest Encryption.

View Data at Rest Encryption settings (physical deployments only)

View Data at Rest Encryption settings.

Format

```
/prot/encrypt show
```

Example

The following command lists the Data at Rest Encryption settings on the system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/encrypt show -detail
```

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

1:     Encryption mode        = Controller Based Encryption
       Encryption status      = Encrypted
       Percent encrypted      = 100.00%
       Backup keystore status = Backup keystore operation complete
       KMIP status            = Enabled
```

Change encryption setting for KMIP support (physical deployments only)

When encryption and KMIP support are enabled, the storage system interacts with external key management servers that are KMIP compliant for key management associated with the Data at Rest Encryption feature. When encryption is enabled and KMIP support is disabled, the storage system interacts with an internal key management server for key management.

Format

```
/prot/encrypt set -kmipEnabled {yes | no}
```

Action qualifiers

Qualifier	Description
`-kmipEnabled`	Specifies whether to enable or disable KMIP support. Valid values are: • `yes` • `no`

Example

The following command changes the encryption setting for KMIP support to enabled:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/encrypt set -kmipEnabled yes
```

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

Operation completed successfully.
```

Manage KMIP support (physical deployments only)

KMIP server configuration of the storage system.

Table 129 KMIP attributes

Attribute	Description
`ID`	KMIP server identifier.
`Username`	Username for accessing the KMIP server.
`Password`	Password for accessing the KMIP server.
`Port`	Port number used to establish a connection to a KMIP server.
`Timeout`	Period to establish a connection to a KMIP server. If the system does not receive a reply from the KMIP server before the specified period expires, it stops sending requests.
`Address`	A list of KMIP server addresses separated with comma. The system uses the addresses in the order from left to right.
`State`	A list of KMIP server states (Up, Down, Unknown) separated with comma.

View KMIP settings (physical deployments only)

View settings for KMIP support.

Format

```
/prot/encrypt/kmip show
```

Example

The following command lists the Data at Rest Encryption settings on the system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/encrypt/kmip show
```

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

1:    ID           = kmip_0
      Username     = admin
      Address      = 10.245.95.125
      Port         = 5696
      Timeout      = 300
      State        = Up
```

Change KMIP support settings (physical deployments only)

Change the key management server parameters related to KMIP support.

Format

```
/prot/encrypt/kmip set -username <value> {-passwd <value> | -passwdSecure} [-port <value>] [-timeout <value>] -addr <value>
```

Action qualifiers

Qualifier	Description
`-username`	Specify the username to use to access the KMIP server.
`-passwd`	Specify the password to use to access the KMIP server.
`-passwdSecure`	Specify the password in secure mode - the user will be prompted to input the password and the password confirmation.
`-port`	Specify the port number used by the KMIP server for KMIP communications. Default value is 5696.
`-timeout`	Specify the timeout for the KMIP server in seconds. If the system does not receive a reply from the KMIP server after the specified timeout, it stops sending requests. Default is 30 seconds.
`-addr`	Specify a list of KMIP server addresses to designate as default addresses. Separate the addresses with a comma. The system uses the addresses in the order in which they are typed.

Example
The following command changes the KMIP transport settings:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/encrypt/kmip
set -username skoobee -passwd doobee -port 5696 -timeout 20 -addr
10.245.95.125
```

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

Operation completed successfully.
```

Verify KMIP settings (physical deployments only)

Verify the current connection to the KMIP server.

Format
`/prot/encrypt/kmip verify`

Example
The following command verifies the connection to the KMIP server:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/encrypt/kmip
verify
```

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

Operation completed successfully.
```

CHAPTER 8

Data Mobility

This chapter contains the following topics:

Manage VNX import sessions

A VNX import (migration) session is used to import data from a VNX1 or VNX2 storage system (source) to a remote Unity storage system (target). Two types of VNX imports are available:

- Virtual Data Mover (VDM) and its related file systems import
- Block LUN or Consistency Group (CG) of LUNs import

Each import session is identified by an ID. The Unisphere online help provides more details about storage import.

Note

At any given point in time, only one command is supported on an import session. Before running a new command, ensure that you wait for the existing action on the import session to complete.

The following table lists the attributes for import sessions:

Table 130 Import session attributes

Attribute	Description
`ID`	ID of the import session.
`Name`	Name of the import session.
`Session type`	Type of import session. Valid values are: • `nas` • `block`
`Health state`	Health state of the import session. Valid values are: • `Unknown (0)` — The remote system health cannot be determined. • `OK (5)` — Session is operating normally. • `OK BUT (7)` — Session is in one of the following states: ▪ Session is initialized but paused. ▪ Session is paused to migrate data in initial copy. ▪ Session is paused to sync data in incremental copy. • `Degraded/Warning (10)` — The session failed for one of the following reasons: ▪ Session failed to read some source files. ▪ Session failed to copy file from source to destination. • `Minor failure (15)` — The session failed for one of the reasons listed in Reasons for import session Minor failures. • `Non-recoverable failure (30)` — An error has caused one or more of the following: ▪ Session failed. ▪ Session failed due to an unrecoverable failure in initial copy.

Table 130 Import session attributes (continued)

Attribute	Description
	■ Session failed due to an unrecoverable failure in incremental copy.
`Health details`	Additional health information. See Appendix A, Reference, for details.
`State`	State of the import session. Valid values are: • `Initialized` • `Initial copy` • `Ready to cutover` • `Paused` • `Cutting over` • `Incremental copy` • `Ready to commit` • `Committing` • `Completed` • `Cancelling` • `Cancelled` • `Pending` • `Syncing`
`Progress`	Import session progress. Only supported for NAS import.
`Source system`	Remote system identifier for source system.
`Source resource`	Source resource identifier.
`Target resource`	Target resource identifier. Initialized status: empty. Other statuses: Target resource identifier.

Table 131 Reasons for import session Minor failures

Reasons
Session failed to provision target resource.
Session failed to migrate data in initial copy.
Session failed and paused to migrate data in initial copy.
Session failed to migrate data in initial copy due to connection failure.
Session failed and paused to migrate data in initial copy due to connection failure.
Session failed to migrate data in initial copy due to source IO failure.
Session failed and paused to migrate data in initial copy due to source IO failure.
Session failed to migrate data in initial copy due to target IO failure.
Session failed and paused to migrate data in initial copy due to target IO failure.

Table 131 Reasons for import session Minor failures (continued)

Reasons
Session failed to sync data in incremental copy.
Session failed and paused to sync data in incremental copy.
Session failed to sync data in incremental copy due to connection failure.
Session failed and paused to sync data in incremental copy due to connection failure.
Session failed to sync data in incremental copy due to source IO failure.
Session failed and paused to sync data in incremental copy due to source IO failure.
Session failed to sync data in incremental copy due to target IO failure.
Session failed and paused to sync data in incremental copy due to target IO failure.
Session failed to commit.
Session failed to cancel.
Session syncing failed.
Session syncing failed due to copy file from source to destination.
Session failed to cutover.
Session has configuration failure.
Session failed due to data failure.
Session failed due to connection failure.
Session failed to start.

View import sessions

View details about existing import sessions for both file and block. You can filter on the session ID.

Format

```
/import/session [-id <value> | -active | -completed | -
cancelled] [-type {block | nas}] show
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the import session.
`-active`	Show only active sessions (sessions that are not completed or cancelled).
`-completed`	Show only completed sessions.
`-cancelled`	Show only cancelled sessions.
`-type`	Specifies what type of sessions to show. Valid values are : • `block` • `nas`

Example

The following command displays all existing import sessions on the system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session show
-detail
```

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

1:    ID                                   = import_1
      Name                                 =
import_sess_vdm1_BB0050562C7D2A_FCNCH0972C330D
      Session type                         = nas
      Health state                         = OK (5)
      Health details                       = "The component is
operating normally. No action is required."
      State                                = Initialized
      Progress                             = empty
      Source system                        = RS_65535
      Source resource                      = vdm1
      Target resource                      = nas_1


2:    ID                                   = import_2
      Name                                 = VNX LUN Group 1 import
      Session type                         = block
      Health state                         = OK (5)
      Health details                       = "The component is
operating normally. No action is required."
      State                                = Initial copy
      Progress                             =
      Source system                        = RS_65535
      Source resource                      = LUNGroup1
      Target resource                      = res_1
```

Manage VNX import sessions for block

A block VNX import is the process in which block LUNs or LUN Groups are imported from a VNX1/VNX2 storage system (source) to a remote Unity storage system (target). Block VNX import makes use of the SANCopy feature which must be enabled and configured on the source system.

Each block import session is identified by an ID. The Unisphere online help provides more details about import of block storage.

Note

At any given point in time, only one command is supported on a block import session. Before running a new command, ensure that you wait for the existing action on the block import session to complete.

The following table lists the attributes related to block import sessions:

Table 132 Block import session attributes

Attribute	Description
`ID`	ID of the block import session.
`Name`	Name of the block import session.

Table 132 Block import session attributes (continued)

Attribute	Description
`Health state`	Health state of the block import session. Valid values are: • `Unknown (0)` — The remote system health cannot be determined. • `OK (5)` — Session is operating normally. • `OK BUT (7)` — Session is in one of the following states: ■ Session is initialized but paused. ■ Session is paused to migrate data in initial copy. ■ Session is paused to sync data in incremental copy. • `Degraded/Warning (10)` — The session failed for one of the following reasons: ■ Session failed to read some source files. ■ Session failed to copy file from source to destination. • `Minor failure (15)` — The session failed for one of the reasons listed in Reasons for import sessions Minor failures. • `Non-recoverable error (30)` — An error has caused one or more of the following: ■ Session failed. ■ Session failed due to an unrecoverable failure in initial copy. ■ Session failed due to an unrecoverable failure in incremental copy. **Note** If the migration session is in an error state, the session will not be recoverable. You will need to delete the session and create a new migration session.
`Health details`	Additional health information. See Appendix A, Reference, for details.
`State`	State of the block import session. Valid values are: • `Pending` • `Syncing` • `Paused` • `Ready to cutover` • `Cancelling` • `Cancelled`
`Progress`	Block import session progress.
`Source system`	Remote system identifier for source system.
`Source resource`	Source resource identifier.
`Target resource`	Target resource identifier.

Table 132 Block import session attributes (continued)

Attribute	Description
Estimated remaining bytes	Specifies the current estimated remaining bytes to be transferred for the current import stage. Only supported for block import.
Percent remaining for import	Specifies the percentage of remaining bytes to be imported against the total size of the import resource.
Cutover threshold percentage	When `Percent remaining for import` is below this threshold, the state of the import session changes to `Ready to cutover`.
Throttle	Specifies whether to throttle the import transfer. When throttle is applied, the import session data transfer rate will be throttled back to minimize impact on host I/O operations. When throttle is off, the import session functions at full speed which could impact host I/O latencies. Valid values are: • `yes` • `no`

Create a block import session

Prerequisites

Before creating a block import session, complete the following configuration tasks:

- Create interfaces on both source and target for data transfer.
- Create an import connection to a Unity-based target system.
- Create a block import target (LUN or LUN Group) on the target system.

Format

```
/import/session/block create [-async] [-name <value>] [-throttle {yes | no}] -srcSys <value> -srcRes <value> -lunPoolPairs <value> [-cutoverThreshold <value>] [-hosts <value>] [-importAsVMwareDatastore {yes | no}]
```

Action qualifiers

Qualifier	Description
-async	Run action in asynchronous mode.
-name	Specifies the name of the import session. **Note** If name is not specified, it will be generated in the pattern `import_sess_<srcRes>_<srcSysSerialNumber>_<targetSysSerialNumber>[_<index>]`
-throttle	Specifies whether to throttle the import transfer. Throttle impacts the import speed and host latency for the related LUNs and file systems that are in use on the source and target storage systems. Valid values are:

Qualifier	Description
	• yes • no **Note** Default is to throttle the import transfer, which means that it is throttled at less than the full speed.
-srcSys	Specifies the source system.
-srcRes	Specifies the source resource.
-lunPoolPairs	Specifies the LUN pool pairs. A comma separated list of mappings between the source LUN and the target storage configuration. **Note** Use the format **srcLUN1:tgtPool1,…,…**. Target LUNs will have the same properties as those of the source LUN, such as name, isThin, SP, and size.
-cutoverThreshold	The percentage threshold below which the import session becomes ready to be cutover.
-hosts	Specifies the hosts. A comma separated list of friendly IDs of hosts to give access to target elements.
-importAsVMwareDatastore	Specifies whether the source LUN is to be imported as a VMware datastore (VMFS). This option is only valid for a LUN session and is not valid for a CG session. Valid values are: • yes • no

Example

The following command creates an import session with these settings:

- Import session name is lun_17_import.
- Source storage system is RS_1.
- Source storage resource is 17.
- LUN pool pair is 17:pool_1.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! import/session/block
create -name lun_17_import -srcSys RS_65596 -srcRes 17 -lunPoolPairs
17:pool_1 -importAsVMwareDatastore yes
```

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

ID = import_1
Operation completed successfully.
```

Change import session settings for block

Change the settings for a block import session.

Format

```
/import/session/block -id <value> set [-async] [-name <value>]
[-paused {yes | no} [-throttle {yes | no}] [-cutoverThreshold
<value>]
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the import session.

Action qualifiers

Qualifier	Description
`-async`	Run action in asynchronous mode.
`-name`	Specifies the new name of the import session.
`-throttle`	Specifies whether to throttle the import transfer. Throttle impacts the import speed and host latency for the related LUNs and file systems that are in use on the source and target storage systems. Valid values are: • `yes` • `no` **Note** Default is to throttle the import transfer, which means that it is throttled at less than the full speed.
`-paused`	Specifies whether to pause the import session. Valid values are: • `yes` • `no` **Note** `no` starts or resumes the import session.
`-cutoverThreshold`	Specifies the threshold percentage below which the import session is cutover-ready.

Example

The following command changes the block import session settings for name to newName, the commitThrottle level to 5, and to not apply the throttle:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/
block -id import_1 set -name newName -throttle no -cutoverThreshold 5
```

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

```
Operation completed successfully.
```

Cut over import session for block

Cut over and complete an existing block import session. Cutting over a block import session can be a long and disruptive process. To reduce the period of disruption, set the cutover threshold as small as possible. By decreasing the cutover threshold to a small value, a smaller number of changes will need to be transferred after the application is quiescent. The cutover threshold is a percentage of the LUN size and hence for larger LUNs it is recommended that the cutover threshold be set to a value smaller than the default value of 5 percent. Lastly, cut over an import session only when the session is in the Cutover Ready state. This action ensures that the cutover is performed when the least number of changes has to be transferred.

After cutover completes successfully, host IOs are switched to the target side and the import process completes automatically.

Format

`/import/session/block -id <value> cutover [-async]`

Object qualifier

Qualifier	Description
`-id`	Type the ID of the import session.

Action qualifier

Qualifier	Description
`-async`	Run the action in asynchronous mode.

Example

The following command cuts the import session, import_1, over to the target system:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/block -id import_1 cutover`

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

Operation completed successfully.
```

Cancel a block import session

Cancel an existing block import session.

Format

`/import/session/block -id <value> cancel [-async]`

Object qualifier

Qualifier	Description
`-id`	Type the ID of the import session.

Action qualifier

Qualifier	Description
`-async`	Run the action in asynchronous mode.

Example

The following command commits the block import session, import_1.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/
block -id import_1 cancel
```

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

Operation completed successfully.
```

View import sessions for block

View details about import sessions for block. You can filter on the session ID.

Format

```
/import/session/block [{-id <value> | -active | -completed | -
cancelled}] show
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the import session.
`-active`	Show only active sessions (sessions that are not completed or cancelled).
`-completed`	Show only completed sessions.
`-cancelled`	Show only cancelled sessions.

Example

The following command displays block import sessions on the system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/
block show -detail
```

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

1:    ID                                   = import_2
      Name                                 = VNX LUN Group 1 import
      Session type                         = block
      Health state                         = OK (5)
      Health details                       = "This import session
is operating normally. No action is required."
      State                                = Syncing
      Progress                             = 0%
      Source system                        = RS_65535
      Source resource                      = LUNGroup1
      Target resource                          = res_1
      Estimated remaining bytes                = 47185920 (45 M)
      Percent remaining for import             = 6
      Cutover threshold percent                = 5
      Throttle                                 = no
```

Manage VNX import sessions for file

A Virtual Data Mover (VDM) file import is the process in which a VDM on a VNX1 or VNX2 storage system (source) is imported to a remote Unity storage system (target). The file systems (common log or split log) associated with the VDM are imported to ufs64 file systems on the target storage system.

Each file import session is identified by an ID. The Unisphere online help provides more details about import of VDM file storage.

Note

At any given point in time, only one command is supported on a file import session. Before running a new command, ensure that you wait for the existing action on the file import session to complete.

The following table lists the attributes for file import sessions:

Table 133 File import session attributes

Attribute	Description
`ID`	ID of the file import session.
`Name`	Name of the file import session.
`Health state`	Health state of the import session. Valid values are: • `Unknown (0)`—The remote system health cannot be determined. • `OK (5)`—Session is operating normally. • `OK BUT (7)`—Session is in one of the following states: ■ Session is initialized but paused. ■ Session is paused to migrate data in initial copy. ■ Session is paused to sync data in incremental copy. • `Degraded/Warning (10)`—The session failed for one of the following reasons: ■ Session failed to read some source files. ■ Session failed to copy file from source to destination. • `Minor failure (15)`—The session failed for one of the reasons listed in Table 131 on page 593. • `Non-recoverable error (30)`—An error has caused one or more of the following: ■ Session failed. ■ Session failed due to an unrecoverable failure in initial copy.

Table 133 File import session attributes (continued)

Attribute	Description
	■ Session failed due to an unrecoverable failure in incremental copy. Note If the migration session is in an error state, the session will not be recoverable. You will need to delete the session and create a new migration session.
Health details	Additional health information. See Appendix A, Reference, for details.
State	State of the NAS server import session. Valid values are: • Initialized • Initial Copy • Ready to Cutover • Cutting Over • Incremental Copy • Ready to commit • Commiting • Completed • Cancelling • Cancelled
Progress	Import session progress.
Source system	Remote system identifier for source system.
Source resource	Source resource identifier.
Source import interface	Source import interface identifier for data transfer.
Source file systems imported as VMWare datastore	Source file systems that are imported as VMWare datastore. The value is a list of source file system IDs, in the format of a range (for continuous file system IDs) or a comma separated value (for file systems that are scattered) of source file system IDs. For example, 13,20~25,30.
Source file systems imported with Data Reduction enabled	Source file systems that are imported with data reduction enabled. The value is a list of source file system IDs, in the format of a range (for continuous file system IDs) or a comma separated value (for file systems that are scattered) of source file system IDs. For example, 13,20~25,30.
Source file systems imported with advanced deduplication enabled	Source file systems that are imported with advanced deduplication enabled.

Table 133 File import session attributes (continued)

Attribute	Description
`Target resource`	Target resource identifier.
`Target resource pool`	Target resource containing pool identifier.
`Target file system to pool mapping`	Target resources are only provisioned after you start the import session (by resuming it). Before the target file systems are provisioned (that is, after creation but before being started), the mapping is from a range (for continuous file system IDs) or a comma separated value (for file system IDs that scatter) of source file system IDs to a target pool. For example, 24~26:pool_1; 28,33~36,40:pool_2;50,55:pool_3;78:pool_4. After all the target file systems are provisioned (that is, after the session started), the mapping is from a range (for continuous file system IDs) or a comma separated value (for file system IDs that are scattered) of target file system IDs to a target pool. For example, res_1~res_3:pool_1; res_4~res_9: pool_2;res_10~res_11:pool_3;res_12:pool_4.
`Target import interface`	Target import interface identifier for data transfer.
`Target default production port`	Target production port identifier. The default port on which production interfaces are created.
`Target production interface to port mapping`	Target resources are only provisioned after you start the import session (by resuming it). Before the target production interfaces are provisioned, the mapping is from a list of source production interfaces to a target port. For example, if_6,if_7: spa_iom_0_eth0; if_9:spa_iom_0_eth1. After the target production interfaces are provisioned, the mapping is from a list of target production interfaces to a target port. For example, if_4,if_5:spa_iom_0_eth0; if_7:port spa_iom_0_eth1.
`Target production interface to VLAN mapping`	Target resources are only provisioned after you start the import session (by resuming it). Before the target production interfaces are provisioned, the mapping is from a list of source production interfaces to a target VLAN. For example, if_6: 6; if_9:9. After the target production interfaces are provisioned, the mapping is from a list of target production interfaces to a target VLAN. For example, if_4:4; if_7:7.
`CIFS domain username`	User name for authentication to Windows domain.
`CIFS domain password`	Password for authentication to Windows domain.
`CIFS local administrator username`	User name for authentication to SMB server on the source VDM (before the import session is started). This user account is imported to the destination NAS server.
`CIFS local administrator password`	Password for authentication to SMB server on the source VDM (before the import session is started). This user account is imported to the destination NAS server.

Create a NAS import session

Create a NAS import session.

Note

This command only creates the import session. To start the import session through the UEMCLI, you must run the `/import/session/nas set` command and specify `no` for the action qualifier `-paused`.

Prerequisites

Before creating a NAS import session, complete the following configuration tasks:

- Create interfaces on both the source and target systems for data transfer.
- Create an import connection from the source VNX to the current Unity-based target system.
- Create a target pool.
- If the source VNX system is configured with the code page 8859-1 or 8859-15 for the NFSv3 clients, ensure the code page for the Unity system matches the code page being used on the VNX system. With Unity OE 4.3 and later, the code page of the Unity system can be changed through the `svc_nas {<NAS_server_name> | all} -param -facility vdm -modify codepage -value <value>` service command.

Format

```
/import/session/nas create [-async] [-name <value>] -srcSys
<value> -srcRes <value> -targetResPool <value>< [-
targetImportIf <value>] [-productionIfPortPairs <value>] [-
productionIfVlanPairs <value>] –fsPoolPairs <value>] –
defaultProductionPort <value> [-srcDhsmUsername <value>] [-
srcDhsmPasswd <value>] [-srcDhsmPasswdSecure <value>][-
unixDirectoryService {directMatch | local | nis | ldap |
localThenNis | localThenLdap | none}] [-
srcLocalCifsAdminUsername <value> {-srcLocalCifsAdminPasswd
<value>|-srcLocalCifsAdminPasswdSecure}] [-
srcFsImportedAsVMWareDatastore <value>] [-
srcFsImportedWithDataReductionEnabled <value>] [-
srcFsImportedWithAdvancedDedupEnabled <value>] [-
skipServerParamCheck]
```

Action qualifiers

Qualifier	Description
`-async`	(Optional) Run operation in asynchronous mode.
`-name`	(Optional) Specifies the new name of the import session. **Note** If name is not specified, it will be generated in the pattern `import_sess_<srcRes>_<srcSysSerialNumber>_<targetSysSerialNumber>[_<index>]`
`-srcSys`	Specifies the source (remote) system.

Qualifier	Description
`-srcRes`	Specifies the source resource.
`-targetResPool`	Specifies the default storage pool to store target NAS server configuration information and file systems.
`-targetImportIf`	(Optional) Specifies the target replication interface for the import session.
`-productionIfPortPairs`	(Optional) Specifies the source VDM production interfaces and target port pairs. Values are a comma separated list of mappings between source VDM production interfaces and target ports. **Note** Use the following format: **`source_interface_1:dest_port_1,source_interface_2:dest_port_2`**
`-productionIfVlanPairs`	(Optional) Specifies the source VDM production interface and the target VLAN pairs. Values are a comma separated list of mappings between source VDM production interfaces and target VLAN pairs. **Note** Use the following format: **`source_interface_1:1,source_interface_2:2`**
`-fsPoolPairs`	(Optional) Specifies the source file system IDs and target pool pairs. Values are a comma separate list of mappings between file system IDs and target pool pairs. **Note** Use the format **`sourceFsId1:destination_pool_friendlyId`** (sourceFsid must be an existing supported source file system ID, otherwise validation fails), or **`sourceFsId2~sourceFsId3:destination_pool_friendlyId`** (sourceFsId2 and sourceFsId3 must be existing supported source file system IDs, the other file system IDs between sourceFsId2 and sourceFsId3 do not necessarily need to exist. The create process only takes existing source file system IDs and skips non-existent file system IDs in the range.). For example, for the input **`12:pool_1,15~20:pool_2`**, source file system IDs with 12, 15, and 20 must exist but source file systems with IDs starting from 16 to 19 do not need to exist.
`-defaultProductionPort`	Specifies the target port where NAS server production interfaces will be created by default.
`-srcDhsmUsername`	Specifies the user name for authentication to DHSM service on the source Data Mover. **Note** When the source VDM has FLR-E/C file systems, file import needs to connect to the DHSM service on the source Data Mover. If the DHSM service is configured with basic or digest authentication, the user name needs to be specified.
`-srcDhsmPasswd`	Specifies the password for authentication to the DHSM service on the source Data Mover.
`-srcDhsmPasswdSecure`	Specifies the password for authentication to the DHSM service on the source Data Mover in secure mode.

Qualifier	Description
	Note The user will be prompted to input the password and the password confirmation.
`-unixDirectoryService`	(Optional) Specifies which Unix directory service to import. Directory service is used for querying identity information for Unix (such as UIDs, GIDs, net groups). Valid values are: • `directMatch` - Import source unixDirectoryService to target without any change. • `local` - Use Local files (passwd, group, hosts, netgroup) for querying identity information for Unix. • `nis` - Use NIS for querying identity information for Unix. • `ldap` - Use LDAP for querying identity information for Unix. • `localThinNis` - Use Local files and then NIS for querying identity information for Unix. • `localThinLdap` - Use Local files and then LDAP for querying identity information for Unix. • `none` - Do not use any of Unix directory services.
`-srcLocalCifsAdminUsername`	(Optional) Specifies the user name for authentication to the CIFS server on the source VDM.
`-srcLocalCifsAdminPasswd`	(Optional) Specifies the password for authentication to the CIFS server on the source VDM.
`-srcLocalCifsAdminPasswdSecure`	(Optional) Specifies the password in secure mode. **Note** The user is prompted to input the password and the password confirmation.
`-srcFsImportedAsVMWareDatastore`	(Optional) Specifies what source file systems are imported as VMWare datastore file systems. Values are a comma separated list of source file system IDs with comma separated value of single file system ID or a range of file system IDs; for example, **`sourceFsId1,sourceFsId2~sourceFsId3`**. `sourceFsId1`, `sourceFsId2`, and `sourceFsId3` must be existing supported source file system IDs. The source file systems with IDs between `sourceFsId2` and `sourceFsId3` do not necessarily need to exist. The create process only takes existing source file system IDs and skips non-existent file systems in the range. For example, for input 13,15~20,25, source file systems with ID 13, 15, 20 and 25 must exist; source file systems with IDs starting from 16 to 19 do not need to exist. **Note** If a VNX file system is specified by this option, it should not contain any tree quotas or user quotas.
`-srcFsImportedWithDataReductionEnabled`	(Optional) Specifies which source file systems are imported with data reduction enabled. Values are a comma separated list of source file system IDs with comma separated value of single file system ID or a range of file system IDs; for example, **`sourceFsId1,sourceFsId2~sourceFsId3`**. `sourceFsId1`, `sourceFsId2`, and `sourceFsId3` must be existing supported source file system IDs. The source

Qualifier	Description
	file systems with IDs between sourceFsId2 and sourceFsId3 do not necessarily need to exist. The create logic only takes existing source file system IDs and skips non-existent file systems in the range. For example, for input 13,15~20,25, source file systems with ID 13,15,20 and 25 must exist; source file systems with IDs starting from 16 to 19 do not need to exist.
-srcFsImportedWithAdvancedDedupEnabled	(Optional) Specifies which source file systems are imported with advanced deduplication enabled. Values are a comma separated list of source file system IDs with comma separated value of single file system ID or a range of file system IDs; for example, **sourceFsId1,sourceFsId2~sourceFsId3**. sourceFsId1, sourceFsId2, and sourceFsId3 must be existing supported source file system IDs. The source file systems with IDs between sourceFsId2 and sourceFsId3 do not necessarily need to exist. The create logic only takes existing source file system IDs and skips non-existent file systems in the range. For example, for input 13,15~20,25, source file systems with ID 13,15,20 and 25 must exist; source file systems with IDs starting from 16 to 19 do not need to exist.
-skipServerParamCheck	(Optional) Specifies whether to skip server parameters check (comparison). When selected, the server parameters check is skipped. In silent mode, the check is not skipped. Import session creation compares server parameters between VNX and Unity. When import session creation fails with a Server parameter error, this option allows the creation to proceed. **NOTICE** Skipping the server parameters check could lead to disruptive cutover during import.

Example

The following command creates an import session with these settings:

Note

The source VDM is a NFS-only VDM.

- Import session name is newName.
- Source storage system is RS_1.
- Source storage resource (VDM) is src_vdm_to_migrate.
- Target resource pool is pool_1.
- Target import interface is if_3.
- Source VDM production interface and target port pairs are source_interface_1:spa_iom_0_eth1 and source_interface_2:spa_iom_0_eth0.
- Source file system and target pool pairs are 100~200:pool_2 and 255:pool_3.
- Target port where NAS server production interfaces will be created is spa_iom_0_eth0.
- Migrate the direct match UNIX Directory Service.
- File systems 13, 20 through 25, and 30 are to be imported as VMWare datastore file systems.
- Skip the server parameters check.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! import/session/nas
create -name MyName1 -srcSys RS_1 -srcRes src_vdm_to_migrate -
```

```
targetResPool pool_1 -targetImportIf if_3 -productionIfPortPairs
source_interface_1:spa_iom_0_eth1,source_interface_2:spa_iom_0_eth0 -
fsPoolPairs 100~200:pool_2,255:pool_3 -defaultProductionPort
spa_iom_0_eth0 -unixDirectoryService directMatch -
srcFsImportedAsVMWareDatastore 13,20~25,30 -skipServerParamCheck
```

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

Using '-skipServerParamCheck' option could lead to disruptive
cutover during migration. Do you want to continue?
yes / no: yes
ID = import_1
Operation completed successfully.
```

The following command creates an import session with these settings:

Note

The source VDM is a NFS-only VDM.

- Import session name is newName.
- Source storage system is RS_1.
- Source storage resource (VDM) is src_vdm_to_migrate.
- Target resource pool is pool_1.
- Target import interface is if_3.
- Source VDM production interface and target port pairs are source_interface_1:spa_iom_0_eth1 and source_interface_2:spa_iom_0_eth0.
- Source file system and target pool pairs are 100~200:pool_2 and 255:pool_3.
- Target port where NAS server production interfaces will be created is spa_iom_0_eth0.
- Migrate the direct match UNIX Directory Service.
- File systems 13, 20 through 25, and 30 are to be imported as VMware datastore file systems.
- File systems 14, 22, 25 through 30 are imported as thin.
- File systems 31 and 40 through 45 are imported and have data reduction applied.
- Skip the server parameters check.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! / import/session/nas
create -name MyName -srcSys RS_1 -srcRes src_vdm_to_migrate -
targetResPool pool_1 -targetImportIf if_3 -productionIfPortPairs
source_interface_1:spa_iom_0_eth1,source_interface_2:spa_iom_0_eth0 -
fsPoolPairs 100~200:pool_2,255:pool_3 -defaultProductionPort
spa_iom_0_eth0 -unixDirectoryService directMatch -
srcFsImportedAsVMwareDatastore 13,20~25,30 -srcFsImportedAsThin
14,22,25~30 -srcFsImportedWithDataReductionEnabled 31,40~45 -
skipServerParamCheck
```

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

```
ID = import_1
Operation completed successfully.
```

The following command creates an import session with these settings:

Note

The source VDM is a CIFS-only VDM.

- Import session name is newName.
- Source storage system is RS_1.
- Source storage resource (VDM) is src_vdm_to_migrate.
- Target resource pool is pool_1.
- Target import interface is if_3.
- Source VDM production interface and target port pairs are source_interface_1:spa_iom_0_eth1 and source_interface_2:spa_iom_0_eth0.
- Source file system and target pool pairs are 100~200:pool_2 and 255:pool_3.
- Target port where NAS server production interfaces will be created is spa_iom_0_eth0.
- The user name for authentication to the CIFS server on the source VDM is cifsadmin1
- The password for authentication to the CIFS server on the source VDM is cifspassword1
- File systems 13, 20 through 25, and 30 are to be imported as VMware datastore file systems.
- File systems 14, 22, 25 through 30 are imported as thin.
- File systems 31 and 40 through 45 are imported and have data reduction applied.
- Skip the server parameters check.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! import/session/nas
create -name MyName1 -srcSys RS_1 -srcRes src_vdm_to_migrate -
targetResPool pool_1 -targetImportIf if_3 -productionIfPortPairs
source_interface_1:spa_iom_0_eth1,source_interface_2:spa_iom_0_eth0 -
fsPoolPairs 100~200:pool_2,255:pool_3 -defaultProductionPort
spa_iom_0_eth0 -srcFsImportedAsVMWareDatastore 13,20~25,30 -
srcLocalCifsAdminUsername cifsadmin1 -srcLocalCifsAdminPasswd
cifspassword1 -skipServerParamCheck
```

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

Using '-skipServerParamCheck' option could lead to disruptive
cutover during migration. Do you want to continue?
yes / no: yes
ID = import_1
Operation completed successfully.
```

Change import session settings for file

Change the settings for a NAS import session.

Format

```
/import/session/nas -id <value> set [-async] [-paused {yes |
no}] -name <value>] [-targetResPool <value>] [-fsPoolPairs
<value>] [-targetImportIf <value>] [-productionIfPortPairs
<value>] [-productionIfVlanPairs <value>] [-
srcLocalCifsAdminUsername <value> {-srcLocalCifsAdminPasswd
<value> | srcLocalCifsAdminPasswdSecure}] [-
srcFsImportedAsVMwareDatastore <value>] [-
srcFsImportedWithDataReductionEnabled <value>] [-
srcFsImportedWithAdvancedDedupEnabled <value>]}
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the import session.

Action qualifiers

Qualifier	Description
`-async`	Run action in asynchronous mode.
`-name`	Specifies the new name of the import session.
`-paused`	Specifies whether to pause the session. Valid values are: • `yes` • `no` **Note** `no` starts or resumes the import session.
`-targetResPool`	Specifies the new pool for the target resource. Applicable only when the session status is Initialized or the target NAS server provision fails.
`-fsPoolPairs`	Specifies the source file system IDs and target pool pairs. Applicable only when the session status is Initialized or the target file system provision fails.
`-targetImportIf`	Specifies the new target migration interface. Applicable only when the session status is Initialized or the target NAS server provision fails.

Qualifier	Description
`-productionIfPortPairs`	Specifies the source VDM production interface and target port pairs. Applicable only when the session status is Initialized or the target production interface creation fails.
`-productionIfVlanPairs`	Specifies the source VDM production interface and the target VLAN pairs. Applicable only when the session status is Initialized or the target production interface creation fails.
`-srcLocalCifsAdminUsername`	Specifies the user name for authentication to the CIFS server on the source VDM.
`-srcLocalCifsAdminPasswd`	Specifies the password for authentication to the CIFS server on the source VDM.
`-srcLocalCifsAdminPasswdSecure`	Specifies the password in secure mode. **Note** The user is prompted to input the password and the password confirmation.
`-srcFsImportedAsVMWareDatastore`	Specifies what source file systems are imported as VMware datastore file systems. Only applies to file import when the session is initialized. **Note** If a VNX file system is specified by this option, it should not contain any tree quotas or user quotas.
`-srcFsImportedWithDataReductionEnabled`	Specifies which source file systems are imported with data reduction enabled. Only applies to file import when the session is initialized.
`-srcFsImportedWithAdvancedDedupEnabled`	Specifies which source file systems are imported with advanced deduplication

Qualifier	Description
	enabled. Only applies to file import when the session is initialized.

Example

The following command changes the NAS import session settings:

Note

This command only makes changes to the import session configuration. To resume (start) the import session through the UEMCLI, you must run the `/import/session/nas set` command and specify `no` for the action qualifier `-paused`.

---

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/nas -id import_1 set -name newName -targetResPool pool_2 -targetImportIf if_3 -productionIfPortPairs source_interface_1:spa_iom_0_eth1,source_interface_2:spa_iom_0_eth0 -fsPoolPairs 100~200:pool_2,255:pool_3 -srcFsImportedAsVMWareDatastore 17~20 -srcFsImportedWithDataReductionEnabled 31,40~45

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

Operation completed successfully.
```

Start or resume an import session

Once an import session is created and optionally modified, it remains in the initialized state until it is started (or resumed). The following command starts (or resumes) the example NAS import session:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/nas -id import_1 set -paused no

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

Operation completed successfully.
```

Cutover import session for file

Cut over an existing NAS import session. Cutting over a session switches the active host IOs to the target side and initiates the incremental data synchronization from the source to the target.

Format

`/import/session/nas -id <value> cutover [-async] [-netbiosName <value>] [-cifsServerName <value> -domainUsername <value> {-domainPasswd <value> | -domainPasswdSecure}]`

Object qualifier

Qualifier	Description
-id	Specifies the ID of the import session.

Action qualifier

Qualifier	Description
-async	Run the action in asynchronous mode.
-netbiosName	Specifies new NetBIOS name for source the CIFS server.
-cifsServerName	Specifies the new name for the source CIFS server after the cutover. SMB (CIFS) server name must be unique on the network. **Note** If not specified, the default name for renaming the source CIFS server is the original CIFS server name prefixed with an underscore (_).
-domainUsername	Specifies the domain administrator name. This name is required for renaming the source CIFS server and joining it to the Active Directory. (Used for AD-joined CIFS server migration only)
-domainPasswd	Specifies the domain user password.
-domainPasswdSecure	Specifies the password in secure mode. **Note** The user is prompted to input the password and the password confirmation.

Example 1

The following command cuts the NFS import session, import_1, over to the target system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/nas
-id import_1 cutover
```

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

Operation completed successfully.
```

Example 2

The following command cuts the SMB import session, import_1, over to the target system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/nas -id import_1 cutover -cifsServerName cifs1 -domainUsername user1 -domainPasswd password1
```

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

Operation completed successfully.
```

Commit import session for file

Commit an existing NAS import session. Committing a session completes the import process.

Format

```
/import/session/nas -id <value> commit [-async]
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the import session.

Action qualifier

Qualifier	Description
`-async`	Run the action in asynchronous mode.

Example

The following command commits the import session, import_1.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/nas -id import_1 commit
```

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

Operation completed successfully.
```

Cancel a NAS import session

Cancel an existing NAS import session.

Format

```
/import/session/nas -id <value> cancel [-async] [-domainUsername <value> {-domainPasswd <value> | -domainPasswdSecure}] [-skipSourceRestore]
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the import session.

Action qualifier

Qualifier	Description
-async	Run the action in asynchronous mode.
-domainUsername	Specifies the domain user with administrative rights to update the AD (not necessary for standalone CIFS server).
-domainPasswd	Specifies the domain user password (not necessary for standalone CIFS server).
-domainPasswdSecure	Specifies the password in secure mode (not necessary for standalone CIFS server). **Note** The user is prompted to input the password and the password confirmation.
-skipSourceRestore	Skip source VDM restore. When specified, the source VDM restore operations are skipped. Normally, the cancel action stops the import transport, deletes the corresponding destination resources, and restores the source VDM (turns up the source interfaces attached to the VDM if they are turned down during cutover and deletes internal export options created by the import for import transport).

Example

The following command cancels the NAS import session, import_1.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/nas
-id import_1 cancel
```

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

Operation completed successfully.
```

View import sessions for file

View details about import sessions for file. You can filter on the session ID.

Format

```
/import/session/nas [{-id <value> | -active | -completed | -
cancelled}] show
```

Object qualifier

Qualifier	Description
-id	Type the ID of the import session.
-active	Show only active sessions (sessions that are not completed or cancelled).

Qualifier	Description
`-completed`	Show only completed sessions.
`-cancelled`	Show only cancelled sessions.

Example

The following command displays file import sessions on the system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/nas
show -detail
```

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

1:    ID                                                               = import_1
      Protocol                                                         = NFS
      Name                                                             =
import_sess_vdm1_BB0050562C7D2A_FCNCH0972C330D
      Health state                                                     = OK (5)
      Health details                                                   = "The component is
operating normally. No action is required."
      State                                                            = Initialized
      Progress                                                         =
      Source system                                                    = RS_1
      Source resource                                                  = vdm1
      Source import interface                                          = nas_migration_1
      Source file systems imported as VMware datastore                 = 13,20~25,30
      Source file systems imported with Data Reduction enabled         = 31,40~45
      Source file systems imported with advanced deduplication enabled = 31,40~45
      Target resource                                                  =
      Target resource pool                                             = pool_1
      Target file system to pool mapping                               = 13~14:pool_1
      Target import interface                                          = if_3
      Target default production port                                   = spa_iom_0_eth0
      Target production interface to port mapping                      =
filesim8129dm2:spa_iom_0_eth0
      Target production interface to vlan mapping                      = filesim8129dm2:1
      CIFS local administrator username                                = admin
      Source DHSM user                                                 = dhsm_admin
```

View import session elements

View details about import status for each element in the active import session, for example, each LUN in a consistency group (CG).

The following table lists the attributes for import session elements:

Table 134 Import session elements attributes

Attribute	Description
Source system	Identifies the source system.
Source resource	Identifies the source resource.
Target resource	Identifies the target resource.

Table 134 Import session elements attributes (continued)

Attribute	Description
Health state	Health state of the import element.
Health details	Additional health information.
Stage	Import data transfer stage. Valid values are: - `Initial sync` - `Incremental sync` - `Final sync`
Iteration	Iteration number in this stage of the import data transfer. This property only applies to the incremental copy stage for LUN import.
Progress	Import progress of current sync iteration.

Format

```
/import/session/element -importId <value> show
```

Object qualifier

Qualifier	Description
`-importId`	Type the ID of the import session.

Example

The following command displays import status for each element in the specified import session:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/
element -importId import_2 show -detail
```

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

1:    Source system   = RS_1
      Source resource = lun1
      Target resource = sv_1
      Health state    = OK (5)
      Health details  = "The component is operating normally. No
action is required."
      Stage           = Incremental Sync
      Iteration       = 4
      Progress        = 10%
      Source system   = RS_1
      Source resource = lun4
      Target Resource = sv_2
      Health state    = OK (5)
      Health details  = "The component is operating normally. No
action is required."
      Stage           = Incremental sync
      Iteration       = 4
      Progress        = 0%
```

Manage generic block resource import sessions

This command imports generic block resources (such as LUNS, volumes, or virtual disks) from a third-party block storage system which provides a Fibre Channel (FC) or iSCSI interface to its block devices (LUNs). It uses the SAN Copy Pull feature running on the local storage system.

If the iSCSI protocol is used, iSCSI connections and connection paths must have been created and configured before you can manage generic import sessions. Refer to the "Manage iSCSI connections" and "Manage iSCSI connection paths" sections in this chapter for more information about configuring iSCSI connections and connection paths.

The following table lists the attributes for import sessions:

Table 135 Import session attributes

Attribute	Description
`ID`	ID of the import session.
`Name`	Name of the import session.
`Description`	Description of the import session.
`Health state`	Health state of the import session. Valid values are: • `Unknown (0)` — The remote system health cannot be determined. • `OK (5)` — Session is in one of the following states: ▪ Session is operating normally. ▪ Session is completed. ▪ Session is cancelled. • `OK_BUT (7)` — Session is in one of the following states: ▪ Session was recovered on SP reboot. ▪ Session is queued. ▪ Session is paused. • `Degraded/Warning (10)` — Session is in one of the following states: ▪ Auto-recovery is in progress. ▪ Recovery on SP reboot. ▪ Waiting on LUN trespass. • `Minor failure (15)` — The session failed either because an SP is down or the session was aborted. • `Major failure` — The session failed for one of the following reasons: ▪ A bad block was encountered on the source block resource. ▪ A restart on auto recovery failed. ▪ The session was halted on an SP reboot. ▪ The destination LUN and the import session are on different SPs.

Table 135 Import session attributes (continued)

Attribute	Description
	■ The destination LUN has been trespassed. • `Critical failure` — The session failed for one of the following reasons: ■ Either the source block resource or destination LUN was not found. ■ Either the source block resource or destination LUN is inaccessible. ■ The source block resource has an invalid connection type. ■ The source block resource failed. ■ The destination LUN is inconsistent. • `Non-recoverable failure (30)` — A non-recoverable error caused the session to fail.
`Health details`	Additional health information. See Appendix A, Reference, for details.
`State`	State of the import session. Valid values are: • `Initialized` • `Pending` • `Running` • `Paused` • `Failed` • `Completed` • `Cancelled`
`SP owner`	Default destination LUN SP owner. Valid values are: • SPA • SPB
`Source system name`	Remote system name provided by the user when the session was created.
`Source LUN WWN`	Source block resource World Wide Name (WWN). The WWN can be passed with the following four prefixes: • wwn. • nna. • wwn-0x. • 0x. It is possible to pass the WWN without any prefixes. For example, the following notations of WWN can be used: • 50060485c5edaa5d—16 hexadecimal chars • 50:06:04:85:c5:ed:aa:5d—Bytes separated by colons

Table 135 Import session attributes (continued)

Attribute	Description
	- 50:6:4:85:c5:ed:aa:5d—Leading nibble of the byte dropped if the nibble is zero - 50-06-04-85-c5-ed-aa-5d—Bytes separated by dashes **Note** If the system rejects the WWN as non-recognizable, you can convert the WWN manually to the Dell EMC Unity system form, such as 60:00:01:6F..
`Target resource`	CLI ID of the destination storage resource.
`Target resource name`	Name of the destination storage resource.
`Target resource type`	Type of the destination resource. Valid values are: - LUN - VMware VMFS
`Size of source`	Size of data to transfer from the source block resource to the destination LUN.
`Size copied`	Total bytes transferred from the source block resource to the destination LUN.
`Size remaining`	Current remaining size in bytes to be transferred from the source block resource to the destination LUN.
`Percent completed`	Percentage of bytes transferred from the source block resource to the destination LUN.
`Start time`	Start time of the copying process.
`Estimated time to complete`	Current estimated time to complete the copying of the source block resource to the destination LUN.
`Throttle`	Reduces CPU load and I/O latency on the destination system. The lower the throttle value, the less impact on the host latency and the longer the import will take. Valid values are: - `Low` - `Medium` - `High` (default)

Create a generic import session

Create an import session for third-party systems.

Format

```
/import/session/generic create [-name <value>] [-descr <value>]
[-srcSystemName <value>] -srcLUNWWN <value> {-targetRes <value>
| -targetResName <value>} [-throttle {Low | Medium | High}] [-
async]
```

Action qualifiers

Qualifier	Description
`-name`	Identifies the import session by unique name. If this name is not specified, it will be generated, using the pattern: `<target LUN CLI ID>-<target LUN name>-<timestamp>`. For example, the name might be generated as `sv_1-LUN01-20180601T160654`.
`-descr`	Specifies the import session description.
`-srcSystemName`	Remote third-party system name. If this name is not specified, the option is left empty and the session cannot be tracked by the remote system name.
`-srcLUNWWN`	Specifies the WWN of the source LUN. The WWN can be passed with the following four prefixes: • wwn. • nna. • wwn-0x. • 0x. It is possible to pass the WWN without any prefixes. For example, the following notations of WWN can be used: • 50060485c5edaa5d—16 hexadecimal chars • 50:06:04:85:c5:ed:aa:5d—Bytes separated by colons • 50:6:4:85:c5:ed:aa:5d—Leading nibble of the byte dropped if the nibble is zero • 50-06-04-85-c5-ed-aa-5d—Bytes separated by dashes **Note** If the system rejects the WWN as non-recognizable, you can convert the WWN manually to the Dell EMC Unity system form, such as 60:00:01:6F..
`-targetRes`	CLI ID of the destination storage resource.
`-targetResName`	Name of the destination storage resource.
`-throttle`	Specifies the import session throttle value. Valid values are: • `Low` • `Medium` • `High` (default)

Qualifier	Description
	Note You can change the Throttle setting when a session is running or paused. Only the `/import/session/generic show -detail` CLI command output will reflect this change when the session is running. However, after the session is completed, that command's output reflects the Throttle value that was set when the session was created, and not the changed value.
`-async`	Run the operation in asynchronous mode.

Example

The following command creates an import session.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/
generic create -name lun_17_import -srcSystemName MyOldGranSystem -
srcLUNWWN 06:00:00:00:05:00:00:00:01:00:00:00:00:00:00:03 -targetRes
sv_1 -throttle High
```

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

ID = glimp_1
Operation completed successfully.
```

View generic import session settings

View details about existing import sessions for third-party systems.

Format

```
/import/session/generic [{-id <value> | -name <value> | -
srcSystemName <value> | -active | -running | -paused | -failed
| -pending | -completed | -cancelled}] show
```

Object qualifiers

Qualifier	Description
`-id`	Type the ID of the import session.
`-name`	Type the unique name for the import session.
`-srcSystemName`	Third-party system name provided by the user at import session creation.
`-active`	Show only active sessions (all sessions that are running, paused, failed, or pending).
`-running`	Show only running sessions.
`-paused`	Show only paused sessions.
`-failed`	Show only failed sessions.
`-pending`	Show only pending sessions.

Qualifier	Description
`-completed`	Show only completed sessions.
`-cancelled`	Show only cancelled sessions.

Example

The following command displays all import sessions on the system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/
generic show -detail
```

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

1:     ID                           = gen_import_1
       Name                         = Session_for1527875375
       Description                  =
       Health state                 = OK (5)
       Health details               = "The generic LUN import session
is running normally."
       State                        = Running
       SP owner                     = SPB
       Trespassed                   = no
       Source system name           =
       Source LUN WWN               = 60:06:01:60:0B:10:3D:
00:80:84:11:5B:3A:20:8E:6A
       Target resource              = sv_23
       Target resource name         =
destLun_Compression_Disabled_TLU_1_Standalone
       Target resource type         = LUN
       Size of source               = 21474836480 (20.0G)
       Size copied                  = 408944640 (390.0M)
       Size remaining               = 21065891840 (19.6G)
       Percent completed            = 1%
       Start time                   = 2018-06-01 17:50:03
       Estimated time to complete   = 2018-06-02 01:32:58
       Throttle                     = Low

2:     ID                           = gen_import_2
       Name                         = Session_for1527875405
       Description                  =
       Health state                 = OK (5)
       Health details               = "The generic LUN import session
is running normally."
       State                        = Running
       SP owner                     = SPA
       Trespassed                   = no
       Source system name           =
       Source LUN WWN               = 60:06:01:60:0B:10:3D:00:8A:
84:11:5B:55:AD:35:5D
       Target resource              = sv_24
       Target resource name         = destLun_DLU_1_Ds
       Target resource type         = VMware VMFS
       Size of source               = 21474836480 (20.0G)
       Size copied                  = 81264640 (77.5M)
       Size remaining               = 21393571840 (19.9G)
       Percent completed            = 0%
       Start time                   = 2018-06-01 17:50:39
       Estimated time to complete   = 2018-06-01 19:14:35
       Throttle                     = Low
```

Change generic import session settings

Changes the existing import sessions settings for third-party systems.

Format

```
/import/session/generic {-id <value> | -name <value>} set [-newName <value>] [-descr <value>] [-srcSystemName <value>] [-throttle <value>] [-async]
```

Object qualifiers

Qualifier	Description
`-id`	Type the ID of the import session.
`-name`	Type the unique name for the import session.

Action qualifiers

Qualifier	Description
`-newName`	Specifies the new name of the import session.
`-descr`	Specifies the import session description.
`-srcSystemName`	Remote third-party system name. If this name is not specified, the option is left empty and the session cannot be tracked by the remote system name.
`-throttle`	Specifies the import session throttle value. Valid values are: • `Low` • `Medium` • `High` **Note** You can change the Throttle setting when a session is running or paused. Only the /import/session/generic show -detail CLI command output will reflect this change when the session is running. However, after the session is completed, that command's output reflects the Throttle value that was set when the session was created, and not the changed value.
`-async`	Run the operation in asynchronous mode.

Example

The following command changes the import session settings for name to newName:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/generic -id gen_import_1 set -name newName
```

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

Operation completed successfully.
```

Pause a generic import session

Pauses a running third-party system import session.

Format

```
/import/session/generic {-id <value> | -name <value>} pause [-async]
```

Object qualifiers

Qualifier	Description
`-id`	Type the ID of the import session.
`-name`	Type the unique name for the import session.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.

Example

The following command pauses the "gen_import_1" import session:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/generic -id gen_import_1 pause
```

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

Operation completed successfully.
```

Resume a generic import session

Resumes running a third-party system import session.

Format

```
/import/session/generic {-id <value> | -name <value>} resume [-async]
```

Object qualifiers

Qualifier	Description
`-id`	Type the ID of the import session.
`-name`	Type the unique name for the import session.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.

Example

The following command resumes the "gen_import_1" import session:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/
generic -id gen_import_1 resume
```

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

Operation completed successfully.
```

Cancel a generic import session

Cancels an existing active or failed third-party system import session.

Note

Once an import session has been cancelled, it cannot be restarted.

Format

```
/import/session/generic {-id <value> | -name <value>} cancel [-
async]
```

Object qualifiers

Qualifier	Description
`-id`	Type the ID of the import session.
`-name`	Type the unique name for the import session.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.

Example

The following command cancels the "gen_import_1" import session:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/
generic -id gen_import_1 cancel
```

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

Operation completed successfully.
```

Restart a generic import session

Restarts a failed third-party system import session, once the cause of the failure has been fixed. The session restarts and copies data from the last block address saved in a checkpoint. However, if the Throttle value was changed while the session was running, the Throttle value that was set when the initial session was created is used, and not the changed value.

Format

```
/import/session/generic {-id <value> | -name <value>} restart
[-async]
```

Object qualifiers

Qualifier	Description
`-id`	Type the ID of the import session.
`-name`	Type the unique name for the import session.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.

Example

The following command restarts the "gen_import_1" import session:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/
generic -id gen_import_1 restart
```

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

Operation completed successfully.
```

Delete a generic import session

Deletes a specified cancelled or completed third-party system import session. The delete operation erases all historical data for the specified import session.

Format

/import/session/generic {-id *<value>* | -name *<value>*} delete [-async]

Object qualifiers

Qualifier	Description
`-id`	Type the ID of the import session.
`-name`	Type the unique name for the import session.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.

Example

The following command deletes the "gen_import_1" import session:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/
generic -id gen_import_1 delete
```

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

```
HTTPS connection

Operation completed successfully.
```

Manage LUN Move sessions

Use the LUN Move feature when you need to move existing LUNs in the system, such as between pools for load balancing, to take advantage of newly purchased spindles, or to enable data reduction (for either newly-written data or both newly-written data and existing data) on a thin LUN in an All Flash pool. Note that if you choose to apply data reduction to existing data, the LUN data is moved within the same pool.

If you move a LUN that:

- Has not had data reduction applied, it is moved as uncompressed.
- Has had data reduction applied, and it is being moved to an All Flash pool, it is moved as compressed. If you are not moving it to an All Flash pool, it is moved as uncompressed.
- Not thin, it is moved as not thin.
- Thin, it is moved as thin.

The following table lists the attributes for moving LUNs:

Table 136 LUN move attributes

Attribute	Description
`ID`	ID of the move session.
`Source resource`	Storage resource for the source.
`Source member LUN`	Source member LUN, if the storage resource is a LUN group.
`Destination pool`	Pool for the destination.
`State`	Current state that represents the lifecycle of a move session. Value is one of the following: • `Initializing`—Move session is in the process of initializing. • `Queued`—Move session is queued to run. The system begins the data transfer when sufficient resources are available. • `Running`—Indicates that the move session is transferring data. • `Failed`—Move session has failed. Consult the move session's health for more details. • `Cancelling`—Indicates that the move session is in the process of being cancelled. • `Cancelled`—Indicates that the move session has been cancelled. • `Completed`—Data transfer for the move session has completed.
`Progress`	Progress of the move session expressed as a percentage.
`Health state`	Health state of the move session. Value is one of the following:

Table 136 LUN move attributes (continued)

Attribute	Description
	• `Unknown`—The move session health cannot be determined. • `OK`—The move session is operating normally. • `Major failure`—One of the following: ▪ The pool went offline and the move cannot continue. Please remove the move session, address the issue, and recreate the move session. ▪ The pool exhausted the space available and the move cannot continue. Please remove the move session, address the issue, and recreate the move session. ▪ The move session encountered an internal error. Please contact your service provider.
`Health details`	Additional health information. See Appendix A, Reference, for health information details.
`Priority`	Priority for the move session. Value is one of the following: • `Idle`—No copy I/O generated. The move session continues to mirror host I/O. • `Low`—Designated for move sessions that have the least priority over other move sessions. • `Below normal`—Designated for move sessions that are slightly less critical than the average or normal move session. • `Normal`—Designated for move sessions that are appropriate for most use cases. This is the default value. • `Above normal`—Designated for move sessions that are slightly more critical than the average or normal move session. • `High`—Designated for move sessions that take the highest priority over other move sessions.
`Average transfer rate`	Average transfer rate of the move session in MB/sec.
`Current transfer rate`	Current transfer rate of the move session in MB/sec.
`Estimated time left`	Estimated time remaining in seconds based on the current transfer rate.

Create a LUN move session

Format

```
/move/session create -srcRes <value> [-srcMemberLun <value>] -
targetPool <value> [-priority {idle | low | below | normal |
above | high} ] [-thin {yes | no}] [-dataReductionEnabled {yes
[-advancedDedupEnabled {yes | no}] | no}] [-async]
```

Action qualifiers

Qualifier	Description
-srcRes	LUN identifier for a standalone source LUN, or a Consistency Group identifier if moving a LUN that is a member of the Consistency Group.
-srcMemberLun	Source LUN identifier if the LUN is a member of a Consistency Group.
-targetPool	Identifier of the destination storage pool where the moved resources will be created.
-priority	Priority of the move session. Valid values are: • idle—Designated for move sessions that continue to mirror the host I/O. • low—Designated for move sessions that have the least priority over other move sessions. • below—Designated for move sessions that are slightly less critical than the average or normal move session. • normal (default)—Designated for move sessions that are appropriate for most use cases. • above—Designated for move sessions that are slightly more critical than the average or normal move session. • high—Designated for move sessions that take the highest priority over other move sessions.
-thin	Indicates whether to create a thin destination. Valid values are: • yes (default) • no
-dataReductionEnabled	Indicates whether to create a destination that will have data reduction applied to it. Valid values are: • yes • no (default)
-advancedDedupEnabled	Indicates whether to create a destination that will have advanced deduplication applied to it. This option only applies when data reduction is enabled. Valid values are: • yes • no (default)
-async	Run the operation in asynchronous mode.

Example 1

The following command creates a move session.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /move/session create
-srcRes sv_1 –targetPool pool_1 -priority above –thin yes -
dataReductionEnabled no
```

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

ID = move_1
Operation completed successfully.
```

Example 2

The following command creates a move session, including the source member LUN ID.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /move/session create
-srcRes res_1 -sourceMemberLun sv_2 -targetPool pool_2 -priority above
-thin yes -dataReductionEnabled yes -advancedDedupEnabled yes
```

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

ID = move_2
Operation completed successfully.
```

View a LUN move session

Format

`/move/session [-id <value>] show`

Object qualifier

Qualifier	Description
`-id`	Type the ID of the move session.

Example

The following command displays details for a LUN move session.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /move/session show -
detail
```

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

1:    ID                     = movesession_1
      Source resource        = sv_1
      Source member LUN      =
      Destination pool       = pool_1
      State                  = Initializing
      Progress               = 0%
      Health state           = OK
      Health details         = "The component is operating normally.
No action is required."
      Priority               = Normal
      Average transfer rate  = 0 MB/s
      Current transfer rate  = 0 MB/s
      Estimated time left    = N/A
```

```
2:    ID                     = movesession_2
      Source resource        = res_1
      Source member LUN      = lun_2
      Destination pool       = pool_2
      State                  = Running
      Progress               = 17%
      Health state           = OK
      Health details         = "The component is operating normally.
No action is required."
      Priority               = Above Normal
      Average transfer rete = 147 MB/s
      Current transfer rate = 232 MB/s
      Estimated time left   = 7m
```

Change LUN move session settings

Format

/move/session -id *<value>* set [-priority {idle | low | below | normal | above | high}] [-async]

Object qualifier

Qualifier	Description
-id	Type the ID of the move session.

Action qualifiers

Qualifier	Description
-priority	Specify the priority of the move session. Valid values are: • idle—Designated for move sessions that continue to mirror the host I/O. • low—Designated for move sessions that have the least priority over other move sessions. • below—Designated for move sessions that are slightly less critical than the average or normal move session. • normal (default)—Designated for move sessions that are appropriate for most use cases. • above—Designated for move sessions that are slightly more critical than the average or normal move session. • high—Designated for move sessions that take the highest priority over other move sessions.
-async	Run the operation in asynchronous mode.

Example

The following command modifies the settings of a move session.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /move/session –id MoveSession_1 set -priority below

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

```
HTTPS connection

ID = MoveSession_1
Operation completed successfully.
```

Delete a LUN move session

Deletes a LUN move session that was completed, cancelled, or failed. You cannot delete a move session that is in progress.

Format

`/move/session -id <value> delete [-async]`

Object qualifier

Qualifier	Description
`-id`	Type the ID of the move session.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.

Example

The following command deletes a move session.

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /move/session –id movesession_1 delete`

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

Operation completed successfully
```

Cancel a LUN move session

Cancels a LUN move session that is in progress.

Format

`/move/session -id <value> cancel [-async]`

Object qualifier

Qualifier	Description
`-id`	Type the ID of the move session.

Action qualifier

Qualifier	Description
`-async`	Run the operation in asynchronous mode.

Example

The following command cancels a move session.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /move/session –id movesession_1 cancel

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

Operation completed successfully.
```

CHAPTER 9

Manage Events and Alerts

This chapter contains 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 drive has faulted, or that the system is low on storage capacity.

In Unisphere, events appear as messages and alerts. The Unisphere CLI displays additional event attributes that provide more detailed event reports than what appears in Unisphere. Configure alert settings on page 643 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 137 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: • `info` – Some event has occurred that does not have an impact on the functioning of the system. • `notice` – An important event has occurred that does not have an impact on the functioning of the system. • `warning` – An error has occurred that you should be aware of but has not had a significant impact on the system. • `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. • `critical` – An error has occurred that has a significant impact on the system and should be remedied immediately.
`Time`	Date and time when the event occurred, in Greenwich Mean Time (GMT).
`Node`	Name of the SP that generated the event. Valid values are: • `spa` • `spb`
`Process`	ID of the system process that generated the event.
`Category`	Event category.

Table 137 Event record attributes (continued)

Attribute	Description
	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.
`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.

Table 138 Alert attributes

Attribute	Description
`ID`	ID of the alert.
`Time`	Date and time (in GMT) when the alert occurred.
`Message`	Alert message.
`Description`	Description of a problem.
`Severity`	Alert severity. Valid values are: • `info` – Some event has occurred that does not have an impact on the functioning of the system. • `notice` – An important event has occurred that does not have an impact on the functioning of the system. • `warning` – An error has occurred that you should be aware of but has not had a significant impact on the system. • `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. • `critical` – An error has occurred that has a significant impact on the system and should be remedied immediately.
`Acknowledged`	Indicates whether or not the alert was acknowledged. Valid values are: • `yes` • `no`

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

The show action command on page 23 explains how to change the output format.

Format

```
/event/log show [-fromTime <value>] [-toTime <value>] [-limit
<value>] [-severity {info | notice | warning | error |
critical}]
```

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. When a new alert comes in, those alerts older than seven days will be cleared..

Format

```
/event/alert/hist show [ -fromTime <value> ] [-toTime <value>]
[-limit <value>] [-acknowledged { yes | no }] [-severity {info
| notice | warning | error | critical}]
```

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.
`-acknowledged`	Type to specify a list of alerts that have or have not been acknowledged. Valid values are: • `yes` • `no`
`-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

```
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:    Id           = alert_3
      Time         = 2016-03-01 17:30:00.309
      Message      = System contact information requires
verification.
```

```
      Description  = "Please verify your system contact
information. This will h
elp your service provider to contact you and quickly respond to any
critical iss
ues. (https://10.108.53.216/help/webhelp/en_US/index.htm?
#vxeuni_c_configure_ale
rt_settings.html)"
      Severity     = info
      Acknowledged = no

2:    Id           = alert_2
      Time         = 2016-03-01 15:19:39.115
      Message      = There are new advisories available for viewing
on the Techn
ical Advisories page.
      Description  = "There are one or more new technical
advisories available f
or viewing on the Technical Advisories page."
      Severity     = notice
      Acknowledged = no

3:    Id           = alert_1
      Time         = 2016-03-01 14:53:05.094
      Message      = System FCNCH0972C35D9 has experienced one or
more problems
that have left it in a degraded state
      Description  = "The system has experienced one or more
failures resulting
in degraded system performance. Check related alerts and fix the
underlying prob
lems. (https://10.108.53.216/help/webhelp/en_US/index.htm?
#vxeuni_t_fix_underlyi
ng_problems.html)"
      Severity     = warning
      Acknowledged = no
```

Acknowledge alerts

Acknowledge specific alerts.

Format

`/event/alert/hist -id <value> ack`

Object qualifier

Qualifier	Description
-id	Type the identifier of the alert you want to acknowledge.

Example

The following command acknowledges alert_2.

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/hist -id alert_2 ack`

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

Operation completed successfully.
```

Delete alerts

Delete specific alerts.

Format

`/event/alert/hist -id <value> delete`

Object qualifier

Qualifier	Description
`-id`	Type the identifier of the alert you want to delete.

Example

The following command deletes alert_3.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/hist -id alert_3 delete
```

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

Operation completed successfully.
```

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 650 provides more details on setting up a destination to receive alerts over SNMP. View event logs and alerts on page 638 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 242.

The following table lists the attributes for alerts:

Table 139 Alert attributes

Attribute	Description
`Language`	Language in which the system sends e-mail alerts.
`E-mail from address`	The email address from which alert emails will be sent.
`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.

Table 139 Alert attributes (continued)

Attribute	Description
	- `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.
`SNMP version`	Version of SNMP that the destination is running.
`SNMP engine ID`	SNMP engine ID for the SNMP destination.
`Show all pool threshold alerts`	Indicates whether the pool space usage percent threshold alerts are enabled. Values are: - `yes` - `no` **Note** Regardless of whether this is enabled, alerts will always be sent for thinly provision pools that are over-subscribed.
`Call home suppression start time`	Date and time when the call home suppression is started.
`Call home suppression end time`	Data and time when the call home suppression ends.

View alert settings

View the settings for how the system handles alerts.

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:     Language                         = en-US
       SNMP severity threshold          = Info
       SNMP version                     = 3.0
       SNMP engine ID                   =
       Show all pool threshold alerts   = no
```

```
        Call home suppression start time= 2017-04-10 00:00:00
        Call home suppression end time   = 2017-04-12 00:00:00
```

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 242.

Format

```
/event/alert/conf set [-emailFromAddr <value>] [-snmpSeverity
{critical|error|warning|notice|info}] [-
showAllPoolThresholdAlerts {yes | no}] [{-
callHomeSuppressionEndTime <value> | -stopCallHomeSuppression}]
```

Action qualifiers

Qualifier	Description
`-emailFromAddrs`	Specify the email address from which alert emails will be sent.
`-snmpSeverity`	Specify the minimal severity of alerts the system will send as SNMP traps. Values are: • `critical` • `error` • `warning` • `notice` • `info`
`-showAllPoolThresholdAlerts`	Specify whether the alert was generated due to an exceeded pool threshold. Valid values are: • `yes` • `no`
`-callHomeSuppressionEndTime`	Specify the date and time when the call home suppression window will end. The total suppression window is the time between the current time and the suppression end time, or the start time and suppression end time for open suppression windows. The suppression window can be in one minute increments between 1 and 48 hours.

Qualifier	Description
	Note Use this option to temporarily suppress call home alerts when you are intentionally performing service actions on your system.
`-stopCallHomeSuppression`	Specify to disable call home suppression.

Example 1

The following command changes these alert settings:

- From address is "from@email.com".
- 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 -emailFromAddr "from@mail.com" -snmpSeverity error
```

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

Operation completed successfully.
```

Example 2

The following command sets the end time for call home alert suppression:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/conf
set -stopCallHomeSuppression
```

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

Operation completed successfully.
```

Configure alert email settings

Specify the alert email settings.

Table 140 Alert email attributes

Attribute	Description
`ID`	Identifier of the alert email configuration.
`Address`	The email address from which alert emails will be sent.
`Severity threshold`	Minimal severity of alerts the system will send emails for. Valid values are: • `critical` — An error has occurred that has a significant impact on the system and should be remedied immediately.

Table 140 Alert email attributes (continued)

Attribute	Description
	- `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.

Configure alert email settings

Configure the "email to" settings for alerts.

Format

```
/event/alert/conf/emailto create -addr <value> [ -severity
{critical | error | warning | notice | info} ]
```

Action qualifier

Qualifier	Description
`-addr`	Type an e-mail address to send alerts to.
`-severity`	Specify the minimum severity of alerts that will trigger emails. Valid values are: - `critical` - `error` - `warning` - `notice` (default) - `info`

Example

This example shows the configuration of the "to" email address of "stuff1@mail.com" and a severity of "info".

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/conf/
emailto create -addr stuff1@mail.com -severity info
```

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

ID = alertEmailConfig_1
Operation completed successfully.
```

Change email alert settings

Change the current configuration for the alert "email to".

Format

```
/event/alert/conf/emailto { -id <value> | -addr <value> } set
[ -newAddr <value> ] [ -severity { info | notice | warning |
error | critical } ]
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the alert configuration you want to modify.
`-addr`	Type the address of the "email to" address for which you would like to change the alert email settings.

Action qualifier

Qualifier	Description
`-newAddr`	Type a new email address to send alerts to.
`-severity`	Type the new the minimum severity of alerts that will trigger emails. Valid values are: • `critical` • `error` • `warning` • `notice` • `info`

Example

The following command changes the alert "email to" address to "stuff1@newmail.com" and specifies the severity level of alerts that will trigger the email is "info".

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/conf/
emailto -addr stuff1@mail.com set -newAddr stuff1@newmail.com -
severity info
```

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

ID = alertEmailConfig_1
Operation completed successfully.
```

View alert email settings

View the "email to" settings for alerts.

Format

```
/event/alert/conf/emailto [{ -id <value> | -addr <value>}] show
```

Object qualifier

Qualifier	Description
`-id`	Type the ID of the alert configuration you want to view.

Qualifier	Description
`-addr`	Type the address of the "email to" address for which you would like view the alert email settings.

Example

This example shows the configuration of all of the alert emails on the system.

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/conf/emailto show`

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

1:     ID                        = alertEmailConfig_1
       Address                   = stuff1@mail.com
       Severity threshold        = Info

2:     ID                        = alertEmailConfig_2
       Address                   = stuff2@mail.com
       Severity threshold        = Notice

3:     ID                        = alertEmailConfig_3
       Address                   = stuff3@mail.com
       Severity threshold        = Notice
```

Test email alert settings

Send a test email to all of the email addresses configured to receive alert notifications.

Format

`/event/alert/conf testEmailAlert`

Example

The following example demonstrates how to test alert email settings.

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/conf testEmailAlert`

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

Operation completed successfully.
```

Delete email alert settings

Delete alert email configurations.

Format

`/event/alert/conf/emailto -id <value> delete`

Object qualifier

Qualifier	Description
`-id`	Type the ID of the alert configuration you want to delete.

Example

The following command changes the alert "email to" address to "stuff1@newmail.com" and specifies the severity level of alerts that will trigger the email is "info".

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/conf/emailto -id alertEmailConfig_1 delete`

```
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 141 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.

Table 141 SNMP destination attributes (continued)

Attribute	Description
`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 } } ] } ] | -v2c -community <value> }
```

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

Qualifier	Description
	• `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.
`-v2c`	Specify that an SNMP v2c destination will be created.
`-community`	Specify the SNMP v2c destination community string.

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

The show action command on page 23 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                 = snmp_target_1
      Version            = v3
      Host               = 10.0.1.3
      Port               = 123
      User name          = v3User
      Auth protocol      = None
      Privacy protocol   = None
      Community          =

2:    ID                 = snmp_target_2
      Version            = v2c
      Host               = 10.0.1.3
      Port               = 879
      User name          =
      Auth protocol      =
      Privacy protocol   =
      Community          = v2CommunityStr
```

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 } } ] } ] |
[ -community <value> ] }
```

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.

Qualifier	Description
-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.
-community	Specify the SNMP v2c destination community string.

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 10

Service the System

This chapter contains 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 the system

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 -d 10.0.0.1 -u Local/joe -p MyPassword456! /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 -d 10.0.0.1 -u Local/joe -p MyPassword456! /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. The system should be in the service mode to execute this action.

Format

```
/service/system reinit
```

Example

The following command reinitializes the storage system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /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 be downloaded using the `uemcli -download` command. (See View the switches on page 29).

Format

```
/service/system collect {-serviceInfo [-type {full |
perfAssessment | perfTrace}] | -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.
`-type`	Specify the type of service information to collect. Valid values are: • `full`(default)–Collect the full set of service information. • `perfAssessment`–Collect service information for doing a performance assessment. • `perfTrace`–Collect service information for doing a trace. • `minimum`—Collect a minimum set of service information (log files only).
`-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 1

The following command collects information about the system and saves it to a file:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /service/system
collect -serviceInfo
```

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

```
Operation completed successfully.
```

Example 2
The following command collects service information about system performance and saves it to a file.

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /service/system collect -serviceInfo -type perfAssessment`

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

Operation completed successfully.
```

Manage core dump files

Manage the list of core dump files, which contain system information used by support for troubleshooting.

Core dump files are generated by the system whenever there is an SP failure. Core dump files are used by support to help troubleshoot and resolve issues.

Table 142 Core dump attributes

Attribute	Description
`ID`	Indicates the unique identifier of the core dump file.
`Name`	Name of the core dump file.
`Creation time`	Date and time when the core dump file was generated.
`File size`	Total size of all the core dump files in the dump folder.

View core dumps

View a list of core dump files generated by the system for both SPs. The files may be downloaded using the `uemcli -download` command. (See View the switches on page 29).

Format
`/service/system/dump [-id <value>] show`

Object qualifier

Qualifier	Description
`-id`	Indicates the unique identifier of the core dump file.

Example
The following command shows a list of the system core dumps.

```
uemcli -d 10.0.0.1 -u local/serviceuser -p Password /service/system/
dump -id "mspb:logDaemon_:2017-03-15_07_34_54_878_logDaemon.x" show
```

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

1:     ID            = mspb:logDaemon_:
2017-03-15_07_34_54_878_logDaemon.x
       Name          =
logDaemon_dump_spb_FCNCH097052190_2017-03-15_07_34_54_878_logDaemon.
x_dir
       Creation time = 2017-03-15 07:34:54.000
       File size     = 126MB
```

Delete core dumps

Delete a core dump file from the list of core dumps generated by the system.

Format

`/service/system/dump {-id <value>} delete`

Object qualifier

Qualifier	Description
`-id`	Specify the unique identifier of the core dump file to be deleted.

Example

The following command deletes a core dump by specifying its name.

```
uemcli -d 10.0.0.1 -u local/serviceuser -p Password /service/system/
dump -id mspa:CP_:2016-06-22_15_13_20_19151_ECOM delete
```

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

Operation completed successfully.
```

Manage 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:

Qualifier	Description
	- yes - no

Example

The following command enables SSH access to the system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /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 -d 10.0.0.1 -u Local/joe -p MyPassword456! /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 -d 10.0.0.1 -u Local/joe -p MyPassword456! /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 -d 10.0.0.1 -u Local/joe -p MyPassword456! /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 -d 10.0.0.1 -u Local/joe -p MyPassword456! /service/sp -id spa reimage
```

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

Operation completed successfully.
```

CHAPTER 11

Manage Metrics

This chapter contains 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 143 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` (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

Use the show action command 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 (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` **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 yes

```
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 144 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

Use the show action command 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. **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 1

The following command displays all available metric service settings for the system:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/metric show`

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

1:   Path          = sp.*.cifs.global.basic.readsRate

2:   Path          = sp.*.cifs.global.basic.totalCallsRate

3:   Path          = sp.*.cifs.global.basic.writeAvgSize
```

Example 2

The following command displays all available metric service settings for the system with additional details:

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/metric show -detail`

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

1:     Path          = sp.*.blockCache.global.summary.cleanPages
       Description   = Number of Clean Pages on SP, based on a
logical
                                    64 KB page size
       Type          = fact
```

```
      Unit         = Count
      Availability = real-time

2:    Path         = sp.*.blockCache.global.summary.dirtyBytes
      Description  = Amount of Dirty Data (MB) on SP
      Type         = fact
      Unit         = MB
      Availability = historical, real-time

3:    Path         = sp.*.blockCache.global.summary.dirtyPages
      Description  = Number of Dirty Pages on SP, based on a
logical
                     64 KB page size
      Type         = fact
      Unit         = Count
      Availability = real-time
```

Example 3

The following command displays all available real-time metric service settings for the system:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/metric -
availability real-time show
```

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

439:  Path = sp.*.storage.pool.*.sizeTotal

440:  Path = sp.*.storage.pool.*.sizeUsed

441:  Path = sp.*.storage.pool.*.sizeUsedBlocks

442:  Path = sp.*.storage.pool.*.snapshotSizeSubscribed

443:  Path = sp.*.storage.pool.*.snapshotSizeUsed

444:  Path = sp.*.storage.summary.readBlocksRate

445:  Path = sp.*.storage.summary.readBytesRate

446:  Path = sp.*.storage.summary.readsRate

447:  Path = sp.*.storage.summary.totalBytesRate
```

Example 4

The following command displays the metrics service settings for the metrics with the specified paths:

```
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 145 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 default output appears in a tabular format.

Note

Use the show action command to change the output format.

Format

```
/metrics/value/hist -path <value> show -interval { 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 • `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

Qualifier	Description
	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.

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.

Qualifier Combination	Output

`-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.
`-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".

Example 1

The following command displays the specified individual metric SPA LUN sv_1 every 60 seconds during the query period:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/value/hist
-path sp.spa.storage.lun.sv_1.readsRate show -interval 60 -from
"2014-06-24 02:12:00" -to "2014-06-24 02:1 4 :00"
```

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

Timestamp           |SP        |LUN               |Read
                    |          |                  |Counts/s
--------------------+----------+------------------+--------
2014-06-24 02:12:00 |spa       |sv_1              |   4.001
2014-06-24 02:13:00 |spa       |sv_1              |   2.400
2014-06-24 02:14:00 |spa       |sv_1              |   9.602
```

Example 2

The following command displays the specified metric, associated with a single object type, SPs, every 60 seconds during the query period:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/value/hist
-path sp.*.cpu.summary.utilization show -interval 60 -from "2014-06-24
02:57:00" -to "2014-06-24 02:59:10"
```

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

Timestamp           |SP        |summary
                    |          |CPU
                    |          |Util %
--------------------+----------+-------
2014-06-24 02:57:00 |spa       |  12.62
                    |spb       |  32.46
```

```
2014-06-24 02:58:00 |spa       |  13.06
                    |spb       |  19.75
2014-06-24 02:59:00 |spa       |  13.44
                    |spb       |  32.47
```

Example 3

The following command displays the specified metric, associated with two object types, SPs and LUNs, every 60 seconds during the query period:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/value/hist -path sp.*.storage.lun.*.readsRate show -interval 60 -from "2014-06-24 02:59:00" -to "2014-06-24 03:01:00"

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

Timestamp           |SP        |LUN               |Read
                    |          |                  |Counts/s
--------------------+----------+------------------+--------
2014-06-24 02:59:00 |spa       |sv_1              |   0.050
                    |spa       |sv_2              |       0
                    |spb       |sv_1              |       0
                    |spb       |sv_2              |   0.033
2014-06-24 03:00:00 |spa       |sv_1              |   0.467
                    |spa       |sv_2              |       0
                    |spb       |sv_1              |       0
                    |spb       |sv_2              |   0.117
2014-06-24 03:01:00 |spa       |sv_1              |   0.833
                    |spa       |sv_2              |       0
                    |spb       |sv_1              |       0
                    |spb       |sv_2              |   0.467
```

Example 4

The following command displays the specified metric, associated with three object types, SPs, pools, and LUNs, every 60 seconds during the query period:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/value/hist -path sp.*.storage.pool.*.lun.*.dataSizeAllocated show -interval 60 -from "2014-06-24 03:04:00" -to "2014-06-24 03:06:00"

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

Timestamp           |SP  |Pool Statistics |LUN   |Data Size
Allocated Bytes
--------------------+----+----------------+------
+--------------------------
2014-06-24 03:04:00 |spa |pool_1          |sv_1  |6442450944
                    |spa |pool_1          |sv_2  |8589934592
                    |spb |pool_1          |sv_1  |6442450944
                    |spb |pool_1          |sv_2  |8589934592
2014-06-24 03:05:00 |spa |pool_1          |sv_1  |6442450944
                    |spa |pool_1          |sv_2  |8589934592
                    |spb |pool_1          |sv_1  |6442450944
                    |spb |pool_1          |sv_2  |8589934592
2014-06-24 03:06:00 |spa |pool_1          |sv_1  |6442450944
                    |spa |pool_1          |sv_2  |8589934592
                    |spb |pool_1          |sv_1  |6442450944
                    |spb |pool_1          |sv_2  |8589934592
```

Example 5

The following command displays metrics, associated with two object types, SPs and LUNs, and an individual metric associated with SPA, every 60 seconds during the query period:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/value/hist -path sp.*.storage.lun.*.readsRate, sp.*.storage.lun.*.writesRate, sp.spa.cpu.summary.utilization show -interval 60 -from "2014-06-24 03:04:00" -to "2014-06-24 03:06:00"

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

Timestamp           |SP     |LUN     |Read     |Write    |SP    |
summary
                    |       |        |Counts/s |Counts/s |      |CPU
                    |       |        |          |        |      |
Util %
--------------------+-------+--------+------+--------+----------
+-------
2014-06-24 03:10:00 |spa    |sv_1    |        0|        0|spa   |
12.63
                    |spa    |sv_2    |    1.050|    9.066|      |
                    |spb    |sv_1    |    0.067|    9.350|      |
                    |spb    |sv_2    |    0.100|    14.95|      |
2014-06-24 03:11:00 |spa    |sv_1    |        0|        0|spa   |
12.56
                    |spa    |sv_2    |    0.700|    26.62|      |
                    |spb    |sv_1    |    0.167|    12.28|      |
                    |spb    |sv_2    |    2.883|    25.65|      |
2014-06-24 03:12:00 |spa    |sv_1    |    0.667|    19.53|spa   |
12.12
                    |spa    |sv_2    |    0.333|    26.87|      |
                    |spb    |sv_1    |    7.066|    3.700|      |
                    |spb    |sv_2    |    7.066|    3.383|      |
```

Example 6

The following command displays the member values for specified metrics every 60 seconds during the query period:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/value/hist -path sp.*.cpu.summary.utilization show -interval 60 -from "2014-06-24 03:14:00" -to "2014-06-24 03:16:00" -flat

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

Timestamp           |spa    |spb
                    |summary|summary
                    |CPU    |CPU
                    |Util % |Util %
--------------------+-------+-------
2014-06-24 03:14:00 |  15.06|  26.78
2014-06-24 03:15:00 |  15.82|  29.39
```

```
2014-06-24 03:16:00 |  15.94|  23.59
```

Example 7

The following command displays the maximum, minimum, and average value for each metric every 60 seconds during the query period:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/value/hist -path sp.*.cpu.summary.utilization show -interval 60 -from "2014-06-24 03:19:00" -to "2014-06-24 03:21:00" -summary

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

Timestamp           |SP        |summary
                    |          |CPU
                    |          |Util %
--------------------+----------+-------
2014-06-24 03:19:00 |spa       |  17.72
                    |spb       |  43.52
2014-06-24 03:20:00 |spa       |  15.35
                    |spb       |  37.82
2014-06-24 03:21:00 |spa       |  15.08
                    |spb       |  36.32

Summary             |SP        |summary
                    |          |CPU
                    |          |Util %
--------------------+----------+-------
Minimum             |spa       |  15.08
                    |spb       |  36.32
Average             |spa       |  16.05
                    |spb       |  39.22
Maximum             |spa       |  17.72
                    |spb       |  43.52
```

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 146 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

Table 146 Real-time metrics attributes (continued)

Attribute	Description
	- `MM` — Minute - `SS` — Second
`Dynamic attributes`	Identifies the object name or metric value.

View real-time metrics settings

View real-time metrics settings. The default output appears in a tabular format.

Note

Use the show action command 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. **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

Qualifier	Description
	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

Objects can come and go at any time, mostly due to object creation and deletion. In flat format, every time a new object is included, the title in tabular or CSV format or the attributes in NVP format is adjusted accordingly and reprinted as necessary on screen. If an object is no longer valid but it already has a column in tabular or CSV format, the column is kept only if its value becomes blank. Otherwise the object is not displayed anymore.

Example 1

The following command displays the specified real-time metric every 10 seconds:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! uemcli /metrics/
value/rt -path sp.*.storage.lun.*.readsRate show -interval 10
```

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

Timestamp           |SP        |LUN               |Read
                    |          |                  |Counts/s
--------------------+----------+------------------+--------
2014-06-24 03:26:10 |spb       |sv_1              |   0.225
2014-06-24 03:26:20 |spb       |sv_1              |   0.200
                    |spb       |sv_2              |   0.100
2014-06-24 03:26:30 |spb       |sv_2              |   0.200
```

Example 2

The following command displays the member values for the specified grouped real-time metric every 10 seconds in comma-separated values (CSV) format:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! uemcli /metrics/
value/rt -path sp.*.storage.lun.*.readsRate show -interval 10 -flat -
output csv
```

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

```
Timestamp,spb sv_1 Read Counts/s
2014-06-24 03:26:10,0.225
Timestamp,spb sv_1 Read Counts/s,spb sv_2 Read Counts/s
2014-06-24 03:26:20,0.200,0.100
2014-06-24 03:26:30,,0.200
```

Example 3

The following command displays the specified real-time metric every 10 seconds name-value pair (NVP) format:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! uemcli /metrics/
value/rt -path sp.*.storage.lun.*.readsRate show -interval 10 -output
nvp
```

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

1: Timestamp = 2014-06-24 03:26:10
   SP        = spb
   Client    = sv_1
   CIFS Read = 0.225

2: Timestamp = 2014-06-24 03:26:20
   SP        = spb
   Client    = sv_1
   CIFS Read = 0.200

3: Timestamp = 2014-06-24 03:26:20
   SP        = spb
   Client    = sv_2
   CIFS Read = 0.100

4: Timestamp = 2014-06-24 03:26:30
   SP        = spb
   Client    = sv_2
   CIFS Read = 0.200
```

CHAPTER 12

Use Cases

This chapter contains the following topics:

Pool use cases

This section describes different CLI use cases for pools.

Create a pool using drives with specific characteristics

This example applies to hybrid Flash arrays, which only support traditional pools.

Retrieve the list of storage profiles

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/profile
-configurable show
```

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

1:    ID                             = profile_22
      Description                    = SAS RAID5
      Drive type                     = SAS
      RAID level                     = 5
      Maximum capacity               = 4611148087296 (4.1T)
      Stripe length                  = Maximum capacity
      Disk group                     = dg_16
      Maximum drives to configure    = 5
      Maximum capacity to configure  = 1884243623936 (1.7T)

2:    ID                             = profile_30
      Description                    = SAS RAID10 (1+1)
      Drive type                     = SAS
      RAID level                     = 10
      Maximum capacity               = 9749818597376 (8.8T)
      Stripe length                  = 2
      Disk group                     = dg_13, dg_15
      Maximum drives to configure    = 10, 10
      Maximum capacity to configure  = 1247522127872 (1.1T),
2954304921600 (2.6T)

3:    ID                             = profile_31
      Description                    = SAS RAID10 (2+2)
      Drive type                     = SAS
      RAID level                     = 10
      Maximum capacity               = 9749818597376 (8.8T)
      Stripe length                  = 4
      Disk group                     = dg_13, dg_15
      Maximum drives to configure    = 8, 8
      Maximum capacity to configure  = 2363443937280 (2.1T),
952103075840 (886.7G)
```

Configure a new pool

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool
create -name MyPool -description "My custom pool" -storProfile
profile_22 -diskGroup dg_16 -drivesNumber 5
```

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

ID = GP_4
Operation completed successfully.
```

Configure a dynamic pool

You can configure dynamic pools for all-Flash models of Unity running OE version 4.2.x or later. New pools created for these models are dynamic pools by default. Dynamic pools implement advanced RAID technology. In dynamic pools, a RAID group is spread across drive extents in multiple drives. The required spare space is also spread across drive extents in multiple drives. When a drive fails, the extents on the failed drive are rebuilt to spare space extents within the pool.

When you configure dynamic pools, you can select different capacity drives from different drive groups with the same Flash drive types to create a tier. The total drive count of the drive type must be at least the stripe width plus one. For example, the total drive count for a RAID 4 + 1 group must be at least 6.

Step 1: View the list of available drive groups
View the list of available drive groups, as shown in the following example:

```
[Request]
Uemcli /stor/config/dg show

[Response]
Storage system address: 127.0.0.1
Storage system port: 443
HTTPS connection

1:    ID                           = dg_2
      Drive type                   = SAS Flash 2
      FAST Cache                   = yes
      Drive size                   = 196971960832 (183.4G)
      Vendor size                  = 200.0G
      Rotational speed             = 0 rpm
      Number of drives             = 12
      Unconfigured drives          = 12
      Capacity                     = 2363663529984 (2.1T)
      Recommended number of spares = 0

2:    ID                           = dg_3
      Drive type                   = SAS Flash 2
      FAST Cache                   = yes
      Drive size                   = 393846128640 (366.7G)
      Vendor size                  = 400.0G
      Rotational speed             = 0 rpm
      Number of drives             = 12
      Unconfigured drives          = 6
      Capacity                     = 4726153543680 (4.2T)
      Recommended number of spares = 0
```

Step 2: View the list of storage profiles
View the list of storage profiles, as shown in the following example:

```
[Request]
Uemcli /stor/config/profile show

[Response]
Storage system address: 127.0.0.1
Storage system port: 443
HTTPS connection

1:    ID                            = profile_1
      Type                          = Dynamic
      Description                   = SAS Flash 2 RAID5 (4+1)
      Drive type                    = SAS Flash 2
      RAID level                    = 5
      Maximum capacity              = 97373737844736 (88.5T)
      Stripe length                 = 5
      Disk group                    =
      Maximum drives to configure   =
      Maximum capacity to configure =
```

Step 3: Configure the dynamic pool
Configure the dynamic pool with the specified drive groups and profiles. Optionally set **-type** to `dynamic` and make sure that the **-drivesNumber** value for each drive type is not less than the drive group's RAID group width plus one:

```
uemcli /stor/config/pool create –name mypool -diskGroup dg_2,dg_3 -
drivesNumber 4,2
-storProfile profile_1 -type dynamic
Storage system address: 127.0.0.1
Storage system port: 443
HTTPS connection

ID = pool_13
Operation completed successfully.[Request]
```

Configure a traditional pool for an all-Flash model

You can configure traditional pools for all-Flash models of Unity running OE version 4.2.x by explicitly setting the `Type` attribute to `traditional`. If you do not set `Type` to `traditional` when you create a pool in the Unisphere CLI, a dynamic pool is created.

Step 1: View the list of storage profiles
View the list of storage profiles, as shown in the following example:

```
[Request]
uemcli /stor/config/profile -traditional -configurable show

[Response]
Storage system address: 127.0.0.1
Storage system port: 443
HTTPS connection

1:    ID                            = tprofile_2
      Type                          = Traditional
      Description                   = SAS Flash 2 RAID5 (8+1)
      Drive type                    = SAS Flash 2
      RAID level                    = 5
      Maximum capacity              = 95010661072896 (86.4T)
      Stripe length                 = 9
      Disk group                    = dg_34, dg_26
      Maximum drives to configure   = 9, 9
      Maximum capacity to configure = 60189403250688 (54.7T),
2232208064512 (2.0T)

2:    ID                            = tprofile_4
      Type                          = Traditional
      Description                   = SAS Flash 2 RAID5
      Drive type                    = SAS Flash 2
      RAID level                    = 5
      Maximum capacity              = 95010661072896 (86.4T)
      Stripe length                 = Maximum capacity
      Disk group                    = dg_34, dg_26
      Maximum drives to configure   = 9, 10
      Maximum capacity to configure = 60189403250688 (54.7T), 
2691354329088 (2.4T)
```

Step 2: Configure the traditional pool

Configure a traditional pool with the specified profile. Make sure you set `-type` to **`traditional`** and that the `-drivesNumber` is a multiple of the RAID group width.

```
uemcli /stor/config/pool create -name test -diskGroup dg_34 -
drivesNumber 9
-storProfile tprofile_2 -type traditional

[Response]
Storage system address: 127.0.0.1
Storage system port: 443
HTTPS connection

ID = pool_6
Operation completed successfully.
```

Add drives to an existing pool

Retrieve the list of existing pools

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /store/config/pool show`

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

1:     ID                = SPL_1
       Name              = Performance
       Description       =
       Free space        = 408944640 (390G)
       Capacity          = 1099511627776 (1T)
       Drives            = 6 x 250GB SAS
       Number of drives  = 6
       Unused drives     = 1
       RAID level        = 5
       System pool       = yes

2:     ID                = SPL_2
       Name              = Capacity
       Description       =
       Free space        = 1319413953331 (1.2T)
       Capacity          = 13194139533312 (12T)
       Drives            = 8 x 2GB NL-SAS
       Number of drives  = 8
       Unused drives     = 0
       RAID level        = 6
       System pool       = yes

3:     ID                = SPL_3
       Name              = Extreme Performance
       Description       =
       Free space        = 209715200 (200M)
       Capacity          = 322122547200 (300G)
       Drive type        = EFD
       Number of drives  = 4
       Unused drives     = 0
       RAID level       = 5
       System pool      = yes
```

Retrieve the list of recommended disk groups for the selected pool

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/dg recom –pool SPL_3

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

1:     ID                        = DG_4
       Drive type                = EFD
       Drive size                = 107374182400 (100G)
       Number of drives          = 4
       Allowed numbers of drives = 4
       Capacity                  = 419430400 (400G)
```

Extend the existing pool

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool –id SPL_3 extend –diskGroup DG_4 –drivesNumber 4

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

ID = SPL_3
Operation completed successfully.
```

File sharing use cases

This section describes different use cases for NAS server file sharing.

Create a NAS server with multiprotocol file sharing

Create the NAS server

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server create -name MyFS1 -sp spa -pool pool_0 -mpSharingEnabled yes -unixDirectoryService ldap -defaultUnixUser fred2 -defaultWindowsUser "fred2"

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

View the NAS server details

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

```
1:    ID                                  = nas_1
      Name                                = MyFS1
      NetBIOS name                        =
      SP                                  = spa
      Storage pool                        = pool_0
      Tenant                            =
      Interface                         =
      NFS enabled                       = yes
      NFSv4 enabled                     = no
      CIFS enabled                      = no
      Workgroup                         =
      Windows domain                    =
      Organization unit                 =
      Multiprotocol sharing enabled     = yes
      Unix directory service            = ldap
      Default Unix username             = fred2
      Default Windows username          = fred2
      Extended Unix credentials enabled = no
      Credentials cache retention       = 15
      Health state                      = OK_But (7)
      Health details                    = "The component cannot
      operate normally - additional configuration steps are
      required. Please ensure configuration of Unix directory
      service. Please ensure configuration of CIFS server."
```

Configure LDAP and upload the Certificate Authority certificate

Configure LDAP

```
uemcli /net/nas/ldap -server nas_1 set -ip 10.0.0.1,10.0.0.1 -port 636
-protocol ldaps authType simple -bindDn
"cn=administrator,cn=User,dc=emc,dc=com" - bindPasswd "Ldap123!" -
baseDn "dc=emc,dc=com"
```

```
Operation completed successfully.
```

Upload the Certificate Authority certificate:

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

```
Operation completed successfully.
```

View the LDAP configuration:

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

```
  [Response]
1:    NAS server          = nas_1
      Servers             = 10.0.0.1, 10.0.0.1
      Port                = 636
      Protocol            = ldaps
      Verify certificate  = yes
      Authentication type = simple
      Bind DN             = cn=administrator,cn=User,dc=emc,dc=com
      Use CIFS account    =
      Principal           =
      Realm               =
      Base DN             = dc=emc,dc=com
      Profile DN          =
```

Configure SMB for the NAS server

Create the interface for the NAS server

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/if create -server nas_1 -port eth0_SPA -addr 10.0.0.1 -netmask 255.255.255.0
```

```
ID = if_0
Operation completed successfully
```

Configure the NAS server as an SMB server

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/cifs create -server nas_1 -domain spb.sspg.lab.emc.com -username Administrator -passwd password1
```

```
ID = cifs_1
Operation completed successfully.
```

View the NAS server health state

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

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

1:    ID                                          = nas_1
      Name                                        =
auto_mig_vdm_6380
      SP                                          = spa
      Storage pool                                = pool_24
      Tenant                                      =
      Interface                                   = if_24
      CIFS enabled                                = yes
      Multiprotocol sharing enabled               = no
      Unix directory service                      = none
      Default Unix username                       =
      Default Windows username                    =
      Username translation                        =
      Health state                                = OK (5)
      Health details                              = "The component
is operating normally. No action is required."
      Type                                        = 64
      Migration Destination                       = yes
      Preferred production interfaces overridden  =
      Preferred production IPv4 interface         = auto
      Preferred production IPv6 interface         = auto
      Preferred backup and DR test IPv4 interface = auto
      Preferred backup and DR test IPv6 interface = auto
      Source preferred production IPv4 interface  =
      Source preferred production IPv6 interface  =
```

Share the file system between NFS and SMB

Create the multiprotocol file system

```
/stor/prov/fs create -name MyFS -server nas_1 -pool pool_0 -size 1000M
-type multiprotocol -accessPolicy native
```

```
ID = res_1
Operation completed successfully.
```

Create an NFS share for the multiprotocol file system

```
/stor/prov/fs/nfs create -name NFSshare -fs res_1 -path / -defAccess
rw
```

```
ID = NFSShare_1
Operation completed successfully.
```

Create an SMB share for the multiprotocol file system

```
/stor/prov/fs/cifs create -name CIFSshare -fs res_1 -path / -comment
"cifsshare"
```

```
ID = SMBShare_1
Operation completed successfully
```

Generate and review the user mapping report

Generate the user mapping report

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server -id
nas_1 update -userMapping -dryRun
```

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

Operation completed successfully.
```

Retrieve the user mapping report

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! uemcli -
download /net/nas/server -id nas_1 -type mappingReport
```

```
Operation completed successfully.

>ls mappingReport_2014-11-18_18-08-00.txt
```

Resource configuration use cases

This section describes use cases for configuring different storage resources.

Identify pool capacity and configure a resource

Identify the SP where the server to be used is located by default

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

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

1:     ID           = nas_1
       Name         = MySFS1
       CIFS enabled = yes
       NFS enabled  = no
       SP           = spa
       Interface    = if_1
```

Check the maximum capacity of the appropriate pool on the identified SP

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                                                = pool_1
   Name                                              = TestPool
   Description                                       =
   Total space                                       = 6266625720320 (5.6T)
   Current allocation                                = 2684354560 (2.5G)
   Remaining space                                   = 6263941365760 (5.6T)
   Subscription                                      = 111967084544 (104.2G)
   Subscription percent                              = 1%
   Alert threshold                                   = 70%
   Drives                                            = 4 x 3.1T SAS Flash 3
   Number of drives                                  = 4
   RAID level                                        = 10
   Stripe length                                     = 2
   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                              = 32768 (32.0K)
   Auto-delete state                                 = Idle
   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 = no
   Auto-delete snapshot space used high water mark   = 25%
   Auto-delete snapshot space used low water mark    = 20%

2: ID                                                = pool_2
   Name                                              = Test1
   Description                                       =
   Total space                                       = 43403328880640 (39.4T)
   Current allocation                                = 57982058496 (54.0G)
   Remaining space                                   = 43345346822144 (39.4T)
   Subscription                                      = 1627792605184 (1.4T)
   Subscription percent                              = 3%
   Alert threshold                                   = 70%
   Drives                                            = 15 x 600.0G SAS;
                                                       2 x 200.0G SAS Flash 2;
                                                       8 x 6.0T NL-SAS;
                                                       2 x 800.0G SAS Flash 2
   Number of drives                                  = 27
   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                                = yes
   Protection size used                              = 2147483648 (2.0G)
   Auto-delete state                                 = Idle
   Auto-delete paused                                = no
   Auto-delete pool full threshold enabled           = no
   Auto-delete pool full high water mark             = 95%
   Auto-delete pool full low water mark              = 85%
   Auto-delete snapshot space used threshold enabled = no
   Auto-delete snapshot space used high water mark   = 25%
   Auto-delete snapshot space used low water mark    = 20%
```

Configure a resource

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 1TB –type nfs

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

ID = res_1
Operation completed successfully.
```

Replication configuration use case

This section describes the use cases for configuring replication for block or file storage resources.

Before you begin

Before you proceed with configuring replication, ensure that you complete the following:

- Create identical storage resources on the source and destination systems.
- Configure replication interfaces for each SP on the source and destination systems.
- On the destination system, the relevant storage resources and NAS servers are individually created with the `-replDest` attribute set to `yes`.
- For file replication, ensure the following:
  - Start with creating identical NAS servers on both the systems, and then create identical file systems.
  - Configure the NAS server on the destination system with a name other than the NAS server name on the source system.

- Configure file systems on the destination system with the same name as the file systems on the source system.

Configure local replication

Note

Local replication is applicable to asynchronous replication only. Local replication is not applicable to synchronous replication.

Replication interfaces and connections do not apply to local replication. When using the CLI or the REST API, once you create the identical source and destination storage resources or NAS servers on the storage system, you can proceed to configure a replication session. When using Unisphere, you only need to create the source storage resources or NAS servers on the storage system. Unisphere does not allow you to create a session with an existing destination. A DR_ is concatenated onto the resource name for local destinations to ensure that the source and destination names on the same system are unique (that is, LUN names need to be unique).

Note the following:

- For a disaster recovery scenario, it is recommended that the destination storage resource and NAS server are configured on a storage pool other than the pool used for the source storage resource and NAS server.
- For a migration scenario, which means migrating the source storage resource and NAS server to a destination storage resource and NAS server on the same pool, use the CLI to configure local replication. The Unisphere GUI does not allow local replication between storage resources and NAS servers on the same pool.

Configure asynchronous replication

Before you begin

If you are configuring asynchronous replication for a tenant, create a pool for the tenant on the destination system that matches the corresponding pool on the source system (if one exists). Then add the tenant to the destination system, using the same UUID and VLANs as the tenant on the source.

If you are configuring asynchronous replication in a coexisting synchronous and asynchronous replication topology, create the asynchronous replication destination NAS server with both the `-replDest` and the `-backupOnly` attributes set to **`yes`**. These attributes must be set to **`yes`** on the asynchronous replication destination NAS server when the source NAS server is synchronous replicated; otherwise, the asynchronous replication session cannot be created.

Procedure

1. Configure the replication interfaces on each SP of the source and destination systems.
2. Configure a replication connection using the **Asynchronous** connection mode.
3. For file storage, create a replication session for the NAS server associated with the file storage.

Note

Storage resources included in a NAS server automatically get replicated when a replication session is first configured for the NAS server. The replication session for the storage resources will inherit the same attributes as the associated replication session of the associated NAS server. For the storage resources you do not want participating in replication, you can choose to remove the associated replication sessions manually.

4. Create a remote replication session for the storage resource.

   Note

   You only need to configure replication interfaces and connections for the first replication session between two systems. The same connection can be used again for subsequent replication sessions between the same systems.

Configure synchronous replication

Note

Only remote replication is supported for synchronous replication.

Procedure

1. Identify the Synchronous Replication Fibre Channel (FC) ports on each system.

   To determine the FC port used for synchronous replication, in the CLI console, run the command `/remote/sys show -detail`. Port information, similar to the following example, will appear in the output:

   ```
   Synchronous FC ports = spb_fc4, spa_fc4
   ```

   For more information, see the *Unisphere CLI User Guide*.

2. Zone the Synchronous Replication FC ports between the systems.

   If the source and destination systems are co-located, instead of zoning, you can choose to use direct-connected FC cables between the SPs.

3. Configure the replication interfaces on each SP of the source and destination systems based on the connection mode you want:

   - For synchronous replication support (**Synchronous** connection mode), use the Synchronous Replication Management Ports on each SP of both the systems.
   - For asynchronous and synchronous replication support (**Both** connection mode), in addition to the replication interfaces for Synchronous Replication Management Ports, configure additional interfaces using the Ethernet Ports on each SP of the source and destination systems.

4. Configure the replication connection between source and destination systems from the source system only.

   - For synchronous replication support, specify the **Synchronous** connection mode.

- For asynchronous and synchronous replication support, specify the **Both** connection mode.

5. Create the synchronous replication session.

   Note

   You only need to configure replication interfaces and connections for the first replication session between two systems. The same connection can be used again for subsequent replication sessions between the same systems.

Create a replication interface

Before you begin

Protection and mobility (import) interfaces can be shared between replication and import. For import, only VDM imports require interfaces. Block imports do not require interfaces.

Protection and mobility (import) interfaces are configured to support VDM imports and must be created prior to creating an import connection. A mobility interface IP address is assigned to SPA and SPB on the target Unity system. Once the mobility interface is configured, you can create the import connection between the Unity system and the VNX system. Mobility interfaces are not used for block import sessions.

Ensure the following:

- The interface port is cabled and connected to a network switch.
- Both SPs are up and running.

Obtain the following information for each Storage Processor (SP):

- IP address associated with the interface (replication or import). Although you can specify an IPv4 or IPv6-based address, ensure that you specify the same type of address for both SPs.
- IP address mask or prefix length that identifies the associated subnet.
- Gateway IP address associated with the interface.
- If applicable, the VLAN ID (between 1 and 4095) you want to associate the interface with.

  Note

  For the network to continue functioning properly, ensure that you set the VLAN ID only when you have configured the network switch port to support VLAN tagging of multiple VLAN IDs.

Ensure that you create replication interfaces on each SP.

Procedure

1. Run the following command to create the interface on SP A:

   ```
   uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/if create
   -type replication -port eth1_spa -addr 10.0.1.1 -netmask
   255.255.255.0 -gateway 10.0.1.0
   ```

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

```
HTTPS connection

ID = IF_1
Operation completed successfully.
```

2. Run the following command to create the interface on SP B:

   uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/if create -type replication -port eth1_spb -addr 10.0.1.2 -netmask 255.255.255.0 -gateway 10.0.1.0

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

ID = IF_2
Operation completed successfully.
```

View interfaces

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                    = iscsi
       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                    = replication
       Port                    = eth1_spa
       VLAN ID                 = 1
       IP address              = 10.0.1.1
       Subnet mask             = 255.255.255.0
       Gateway                 = 10.0.1.0
       SP                      = spa

3:     ID                      = IF_2
       Type                    = replication
       Port                    = eth1_spb
       VLAN ID                 =
       IP address              = 10.0.1.2
       Subnet mask             = 255.255.248.0
       Gateway                 = 10.0.1.0
       SP                      = spb
```

Create a replication connection

Before you begin

Ensure that you have set up relevant replication interface pairs, one on each SP, on the source and destination systems. Obtain the following information:

- For remote replication, the IP address and associated user authentication credentials to connect to the remote system.

- For local replication, the password associated with your user account.
- The connection mode you want to use for the replication: Asynchronous, Synchronous, or Both.

NOTICE

If a replication connection already exists and you plan to add a different mode of file replication, do not attempt to create a new connection. Change the existing replication connection mode to Both. Also, ensure that you have the appropriate interface types configured to support both asynchronous replication (eth2, eth3) and synchronous replication (sync replication mgmt port).

Consider that you want to create an asynchronous replication connection to the remote system with the IP address 10.1.1.1.

Procedure

- Run the following command:

  ```
  uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/sys
  create -addr 10.1.1.1 -srcUsername admin1 -srcPassword Password456!
  -dstUsername admin2 -dstPassword Password986! -connectionType async
  ```

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

  ID = RS_1
  Operation completed successfully.
  ```

View settings for remote storage systems

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

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

1:      ID                    = RS_1
        Name                  = MyTargetSystem
        Address               = 10.1.1.1
        Model                 = Unity 300
        Serial number         = FCNCH01234567A90
        Connection type       = async
        Source interfaces     = N/A
        Local interfaces      = N/A
        Remote interfaces     = N/A
        Operational status    = OK (0x2)
        Health state          = OK (5)
        Health details        = "Communication with the replication
                                 host is established. No action is
                                 required."
        Synchronous FC ports = spb_fc4, spa_fc4
```

Create a replication session for block storage

Before you begin

Complete the following:

- For remote replication:
  - Identify the remote system that will act as the replication destination.
  - Create relevant replication interfaces, replication connection, and a storage resource on the remote system that will act as the destination.
- For local replication, create a storage resource that will act as the destination.
- Determine the replication synchronization mode you want. You can specify asynchronous (async), synchronous (sync), or manual synchronization (manual).
- For asynchronous replication, determine the Recovery Point Objective (RPO) for the replication session.

Procedure

- Run the following command to create a synchronous replication session between the LUN "LUN_1" on the source system and the LUN "LUN_2" located on the remote system "RS_2":

  ```
  uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session
  create -name REP1 -srcRes LUN_1 –dstType remote -dstSys RS_2 –
  dstRes LUN_2 –syncType auto –rpo 0
  ```

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

  ID =
  81604378625_FCNCH097274B3A_0000_81604378627_FCNCH097274B37_0000
  Operation completed successfully.
  ```

Create an asynchronous replication session for file storage

Before you begin

Complete the following:

- For remote replication:
  - Identify the remote system that will act as the replication destination.
  - Create relevant replication interfaces, replication connection, and a storage resource on the remote system that will act as the destination. The storage resource on the destination system must have the same size
- For local replication, create a storage resource that will act as the destination.
- For file replication, create a replication session on the NAS server associated with the file storage.
- For asynchronous replication, determine the Recovery Point Objective (RPO) for the replication session.

NOTICE

If you are configuring asynchronous replication in a coexisting synchronous and asynchronous replication with one source resource topology, create the asynchronous replication destination NAS server with both the `-replDest` and the `-backupOnly` attributes set to **`yes`**. These attributes must be set to **`yes`** on the asynchronous replication destination NAS server when the source NAS server is synchronous replicated; otherwise, the asynchronous replication session cannot be created.

Configure an asynchronous replication session between the NAS servers associated with the file storage, with an RPO set to 2 hours 30 minutes and automatic synchronization. On the source system, the file system "res_7" is associated with NAS server "nas_1". And, the file system "res_8" is associated with NAS server "nas_2" on the remote system.

Procedure

1. Run the following command to create an asynchronous replication session between the NAS servers:

   ```
   uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/
   session create -async -srcRes nas_1 -dstType remote -dstSys RS_2
   -dstRes nas_2 auto -rpo 02h30m
   ```

   ```
   Job ID = N-86
   Operation completed successfully.
   ```

2. Run the following command to create an asynchronous replication session between the file system "res_7" on the source system and the file system "res_8" located on the remote system "RS_2", with an RPO set to 2 hours 30 minutes and automatic synchronization:

   ```
   uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/
   session create -async -srcRes res_7 -dstType remote -dstSys RS_2
   -dstRes res_8 -syncType auto -rpo 02h30m
   ```

   ```
   Job ID = N-89
   Operation completed successfully.
   ```

Create a synchronous replication session for file storage

Before you begin

Complete the following:

- For remote replication:
  - Identify the remote system that will act as the replication destination.
  - Create relevant replication interfaces, replication connection, and a storage resource on the remote system that will act as the destination. The storage resource on the destination system must have the same size.
- For local replication, create a storage resource that will act as the destination.
- For file replication, create a replication session on the NAS server associated with the file storage.

Configure a synchronous replication session between the NAS servers associated with the file storage.

Procedure

1. Run the following command to create a synchronous replication session between the NAS servers:

   uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session create –name MyNSRep1 -srcRes nas_1 –dstType remote –dstSys RS_1 –dstRes nas_1

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

   ID =
   103079215106_FCNCH097274999_0000_103079215106_FCNCH0972749A9_0
   000
   Operation completed successfully.
   ```

2. Run the following command to create a synchronous replication session between file systems on the source system and the remote system:

   uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session create –name MyFSRep1 -srcRes res_1 –dstType remote –dstSys RS_1 –dstRes res_1

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

   ID =
   171798691844_FCNCH097274999_0000_171798691844_FCNCH0972749A9_0
   000
   Operation completed successfully.
   ```

View replication sessions

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                   =
81604378635_FCNCH097274B3A_0000_81604378637_FCNCH097274B37_0000
      Name                 = REP2
      Session type         = nas server
      Synchronization type = auto
      Resource type        = NAS Server
      Destination type     = remote
```

APPENDIX A

Reference

This appendix contains the following topics:

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)"
```