vserver iscsi commands

ONTAP commands

NetApp
February 04, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-cli-97/vserver-iscsi-create.html on February 04, 2026. Always check docs.netapp.com for the latest.

Table of Contents

vserver iscsi commands . . . 1
vserver iscsi create . . . 1
Description . . . 1
Parameters . . . 1
Examples . . . 2
vserver iscsi delete . . . 2
Description . . . 2
Parameters . . . 2
Examples . . . 2
Related Links . . . 2
vserver iscsi modify . . . 3
Description . . . 3
Parameters . . . 3
Examples . . . 4
vserver iscsi show . . . 4
Description . . . 4
Parameters . . . 4
Examples . . . 5
vserver iscsi start . . . 7
Description . . . 7
Parameters . . . 7
Examples . . . 7
Related Links . . . 7
vserver iscsi stop . . . 7
Description . . . 8
Parameters . . . 8
Examples . . . 8
Related Links . . . 8
vserver iscsi command show . . . 8
Description . . . 8
Parameters . . . 8
Examples . . . 9
vserver iscsi connection show . . . 10
Description . . . 10
Parameters . . . 10
Examples . . . 11
vserver iscsi connection shutdown . . . 12
Description . . . 12
Parameters . . . 12
Examples . . . 12
Related Links . . . 13
vserver iscsi initiator show . . . 13
Description . . . 13

Parameters . . . 13
Examples . . . 14
vserver iscsi interface disable . . . 14
Description . . . 14
Parameters . . . 14
Examples . . . 14
vserver iscsi interface enable . . . 15
Description . . . 15
Parameters . . . 15
Examples . . . 15
vserver iscsi interface modify . . . 15
Description . . . 15
Parameters . . . 15
Examples . . . 16
vserver iscsi interface show . . . 16
Description . . . 16
Parameters . . . 16
Examples . . . 17
vserver iscsi interface accesslist add . . . 18
Description . . . 18
Parameters . . . 19
Examples . . . 19
Related Links . . . 19
vserver iscsi interface accesslist remove . . . 20
Description . . . 20
Parameters . . . 20
Examples . . . 20
vserver iscsi interface accesslist show . . . 20
Description . . . 21
Parameters . . . 21
Examples . . . 21
vserver iscsi isns create . . . 21
Description . . . 21
Parameters . . . 22
Examples . . . 22
Related Links . . . 22
vserver iscsi isns delete . . . 22
Description . . . 23
Parameters . . . 23
Examples . . . 23
vserver iscsi isns modify . . . 23
Description . . . 23
Parameters . . . 23
Examples . . . 24
vserver iscsi isns show . . . 24

Description . . . 24
Parameters . . . 24
Examples . . . 25
vserver iscsi isns start . . . 25
Description . . . 26
Parameters . . . 26
Examples . . . 26
vserver iscsi isns stop . . . 26
Description . . . 26
Parameters . . . 26
Examples . . . 26
vserver iscsi isns update . . . 26
Description . . . 26
Parameters . . . 27
Examples . . . 27
vserver iscsi security add-initator-address-ranges . . . 27
Description . . . 27
Parameters . . . 27
Examples . . . 27
vserver iscsi security create . . . 28
Description . . . 28
Parameters . . . 28
Examples . . . 28
vserver iscsi security default . . . 29
Description . . . 29
Parameters . . . 29
Examples . . . 30
Related Links . . . 30
vserver iscsi security delete . . . 30
Description . . . 30
Parameters . . . 30
Examples . . . 31
vserver iscsi security modify . . . 31
Description . . . 31
Parameters . . . 31
Examples . . . 32
Related Links . . . 32
vserver iscsi security prepare-to-downgrade . . . 32
Description . . . 32
Examples . . . 32
Related Links . . . 32
vserver iscsi security remove-initator-address-ranges . . . 32
Description . . . 33
Parameters . . . 33
Examples . . . 33

vserver iscsi security show . . . 33
Description . . . 33
Parameters . . . 33
Examples . . . 35
vserver iscsi session show . . . 36
Description . . . 36
Parameters . . . 37
Examples . . . 39
Related Links . . . 39
vserver iscsi session shutdown . . . 39
Description . . . 39
Parameters . . . 39
Examples . . . 39
Related Links . . . 40
vserver iscsi session parameter show . . . 40
Description . . . 40
Parameters . . . 40
Examples . . . 42
Related Links . . . 42

vserver iscsi commands

vserver iscsi create

Create a Vserver's iSCSI service

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command creates an iSCSI target for a specified Vserver. By default the system creates a default iSCSI target name with the status-admin set to enabled. Until you create an iSCSI service, iSCSI initiators cannot log into the Vserver.

Parameters

`-vserver <Vserver Name>` - Vserver

Specifies the Vserver for the iSCSI service.

`[-target-name <text>]` - Target Name (privilege: advanced)

Specifies a iSCSI target name of a Vserver. This name is unique and is not case sensitive. The target name must conform to this format iqn.1995-08.com.example:string and the following rules:

- Contains up to 128 bytes.
- Contains alphanumeric characters. The period ".", hyphen "-", and colon ":" are acceptable.
- Does not contain the underscore character "_".

`[-target-alias <text>]` - Target Alias

Specifies an iSCSI target alias name of a Vserver. The maximum number of characters for an alias name is 128. The alias default name is the Vserver name.

`[-status-admin {down|up}]` - Administrative Status

Specifies the administrative status of the iSCSI service of a Vserver. If you set this parameter to up, the command creates an iSCSI service with the administrative status of up. If you set this parameter to down, the command creates an iSCSI service with the administrative status of down.

`[-retain-timeout <integer>]` - RFC3720 DefaultTime2Retain Value (in sec) (privilege: advanced)

Specifies the wait time before an active task reassignment is possible after an unexpected connection termination. For example, a value of 0 means that the connection or task state is immediately discarded by the target. The default is 20 seconds.

`[-login-timeout <integer>]` - Login Phase Duration (in sec) (privilege: advanced)

Specifies the login phase duration. The default is 15 seconds.

`[-max-conn-per-session <integer>]` - Max Connections per Session (privilege: advanced)

Specifies the maximum number of connections per session that a target can accept. The default is 4 connections.

[-max-ios-per-session <integer>] - Max Commands per Session (privilege: advanced)

Specifies the maximum number of commands per session that a target can accept. The default is 128 commands per session.

[-tcp-window-size <integer>] - TCP Receive Window Size (in bytes) (privilege: advanced)

Specifies the TCP receive window size (in bytes). The default is 131,400 bytes.

[-f, -force <true>] - Allow Non-Vendor Target Name (privilege: advanced)

Force the command to accept a target name that would normally be rejected as invalid.

Examples

```
cluster1::> vserver iscsi create -vserver vs_1
```

Creates the iSCSI service for Vserver vs_1.

vserver iscsi delete

Delete a Vserver's iSCSI service

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command deletes the iSCSI service from a Vserver.

> You must first disable the service with the command vserver iscsi modify with "-status-admin down" before you can delete the service.

Parameters

-vserver <Vserver Name> - Vserver

Specifies the Vserver for the iSCSI service.

Examples

```
cluster1::> vserver iscsi delete -vserver vs_1
```

Deletes the iSCSI service for Vserver vs_1.

Related Links

- vserver iscsi modify

vserver iscsi modify

Modify a Vserver's iSCSI service

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command modifies the configuration for an iSCSI service.

Modifications take effect immediately after you execute the command. Making modifications to your service can result in traffic loss on a live system. Call technical support if you are unsure of the possible consequences.

Parameters

`-vserver <Vserver Name>` - Vserver

Specifies the Vserver for the iSCSI service.

`[-target-name <text>]` - Target Name (privilege: advanced)

Specifies an iSCSI target name of a Vserver. This name is unique and is not case sensitive. The target name must conform to this format iqn.1995-08.com.example:string and the following rules:

- Contains up to 128 bytes.
- Contains alphanumeric characters. The period ".", hyphen "-", and colon ":" are acceptable.
- Does not contain the underscore character "_".

The iSCSI service must be down in order to change the target name.

{ `[-target-alias <text>]` - Target Alias

Specifies the new target alias of the iSCSI service.

| `[-c, -clear <true>]` - Clear the Target Alias }

Clears the current target alias from the iSCSI service configuration.

`[-status-admin {down|up}]` - Administrative Status

Specifies the configured administrative status of a service. If you set this parameter to up, the iSCSI service begins to accept login requests from iSCSI initiators. If you set this parameter to down, iSCSI initiators cannot log in.

`[-retain-timeout <integer>]` - RFC3720 DefaultTime2Retain Value (in sec) (privilege: advanced)

Specifies the wait time before active task reassignment is possible after an unexpected connection termination. For example, a value of 0 means that the connection or task state is immediately discarded by the target.

`[-login-timeout <integer>]` - Login Phase Duration (in sec) (privilege: advanced)

Specifies maximum time the login phase remains active until the iSCSI target terminates the connection.

[-max-conn-per-session <integer>] - Max Connections per Session (privilege: advanced)

Specifies the maximum number of connections per session that the iSCSI target can accept.

[-max-ios-per-session <integer>] - Max Commands per Session (privilege: advanced)

Specifies the maximum number of commands per session that the iSCSI target can accept.

[-tcp-window-size <integer>] - TCP Receive Window Size (in bytes) (privilege: advanced)

Specifies the TCP receive window size (in bytes).

A change to the TCP receive window size value takes effect for all network interfaces when you restart the iSCSI service for the Vserver as follows:

```
vserver iscsi stop -vserver <vserver name>
vserver iscsi start -vserver <vserver name>
```

If you change an individual network interface from up to down back to up, as follows, the new value for TCP receive window size takes effect for that network interface:

```
network interface modify -vserver <vserver name> -lif <LIF name> -status
-admin down
network interface modify -vserver <vserver name> -lif <LIF name> -status
-admin up
```

[-f, -force <true>] - Allow Non-Vendor Target Name (privilege: advanced)

Force the command to accept a target name that would normally be rejected as invalid.

Examples

```
cluster1::> vserver iscsi modify -vserver vs_1 -status-admin down
```

Modifies the status-admin of the iSCSI service for Vserver vs_1 to down.

vserver iscsi show

Display a Vserver's iSCSI configuration

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command displays the current configuration of the iSCSI service.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Vserver

Selects the iSCSI services for the Vserver that matches the parameter value.

[-target-name <text>] - Target Name

Selects the iSCSI services with a target name that matches the parameter value.

[-target-alias <text>] - Target Alias

Selects the iSCSI services with a target alias that matches the parameter value.

[-status-admin {down|up}] - Administrative Status

Selects the iSCSI services with a configured status that matches the parameter value.

[-retain-timeout <integer>] - RFC3720 DefaultTime2Retain Value (in sec) (privilege: advanced)

Selects the iSCSI services with a wait time that matches the parameter value. The wait time is the amount of time before active task reassignment is possible after an unexpected connection termination.

[-login-timeout <integer>] - Login Phase Duration (in sec) (privilege: advanced)

Selects the iSCSI services with a login phase duration that matches the parameter value.

[-max-conn-per-session <integer>] - Max Connections per Session (privilege: advanced)

Selects the iSCSI services with a maximum connection per session that matches the parameter value.

[-max-ios-per-session <integer>] - Max Commands per Session (privilege: advanced)

Selects the iSCSI services with a maximum number of commands per session that matches the parameter value.

[-tcp-window-size <integer>] - TCP Receive Window Size (in bytes) (privilege: advanced)

Selects the iSCSI services with a TCP receive window size (in bytes) that matches the parameter value.

Examples

```
cluster1::> vserver iscsi show
           Target                              Target
Status
Vserver    Name                                Alias
Admin
---------- ------------------------------- ----------------------------
------
vs_1       iqn.1992-
08.com.example:sn.c7c82a22bf9f11df83e5123478563412:vs.2
                                               vs_1_alias
up
1 entries were displayed.

cluster1::> vserver iscsi show -instance
Vserver: vs_1
                             Target Name: iqn.1992-
08.com.example:sn.c7c82a22bf9f11df83e5123478563412:vs.2

The following is the output of the show command at the advanced privilege
level:
Target Alias: vs_1_alias
                  Administrative Status: up
1 entries were displayed.
```

Displays the output of the show command at the admin privilege level.

```
cluster1::*> vserver iscsi show
           Target                              Target
Status
Vserver    Name                                Alias
Admin
---------- ------------------------------- ----------------------------
------
vs_1       iqn.1992-
08.com.example:sn.c7c82a22bf9f11df83e5123478563412:vs.2
                                               vs_1_alias
up
1 entries were displayed.
```

Displays the output of the show command at the advanced privilege level.

```
cluster1::*> vserver iscsi show -instance
Vserver: vs_1
                              Target Name: iqn.1992-
08.com.example:sn.c7c82a22bf9f11df83e5123478563412:vs.2
                             Target Alias: vs_1_alias
                     Administrative Status: up
RFC3720 DefaultTime2Retain Value (in sec): 20
            Login Phase Duration (in sec): 15
              Max Connections per Session: 4
                       Max I/O per Session: 128
  TCP Window Size all Sessions (in bytes): 131400
```

Displays the detailed entries for all entries.

vserver iscsi start

Starts the iSCSI service

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command starts the iSCSI service of a Vserver. You can also use vserver iscsi modify with "-status-admin up".

Parameters

-vserver <Vserver Name> - Vserver

Specifies the Vserver for the iSCSI service.

Examples

```
cluster1::> vserver iscsi start -vserver vs_1
```

Starts the iSCSI service for Vserver vs_1.

Related Links

- vserver iscsi modify

vserver iscsi stop

Stops the iSCSI service

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

Stops the iSCSI service of a Vserver. This command shuts down all active iSCSI sessions and stops any new iSCSI sessions. You can also use vserver iscsi modify with "-status-admin down".

Parameters

-vserver <Vserver Name> - Vserver

Specifies the Vserver for the iSCSI service.

Examples

```
cluster1::> vserver iscsi stop -vserver vs_1
```

Stops the iSCSI service for Vserver vs_1.

Related Links

- vserver iscsi modify

vserver iscsi command show

Display active iSCSI commands

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command displays the status of active iSCSI commands in an iSCSI session. If you specify an iSCSI command ID, the command shows what commands are active in a session and is useful for initiator debugging.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Vserver

Use this parameter to display a list of active iSCSI commands that match the Vserver name that you specify.

[-tpgroup <text>] - Target Portal Group

Use this parameter to display a list of active iSCSI commands that are within the target portal group.

[-tsih <integer>] - Target Session ID

Use this parameter to display a list of active iSCSI commands that match the target session ID handle that you specify.

[-command-id <integer>] - Command ID

Use this parameter to display a list of active iSCSI commands that match the command ID that you specify.

[-initiator-name <text>] - Initiator Name

Use this parameter to display a list of active iSCSI commands that match the initiator name that you specify.

[-initiator-alias <text>] - Initiator Alias

Use this parameter to display a list of active iSCSI commands that match the initiator alias that you specify.

[-isid <text>] - Initiator Session ID

Use this parameter to display a list of active iSCSI commands that match the initiator session ID that you specify.

[-command-sub-id <integer>] - Command Sub ID

Use this parameter to display a list of active iSCSI commands that match the command sub ID that you specify.

[-command-state <iSCSI Command States>] - Command State

Use this parameter to display a list of active iSCSI commands that match the command state that you specify.

[-command-type {Sequenced|Imm_Taskmgmt|Imm_Other}] - Command Type

If you use this parameter, the command displays a list of active iSCSI commands that contains the specified command type. The command types indicate:

- "Sequenced" — the system processes the commands in sequence
- "Imm_Taskmgmt" — the system processes the commands immediately
- "Imm_Other" — the system processes the commands as queued

Examples

```
cluster1::> vserver iscsi command show -instance -vserver vs_1
server: vs_1
        Target Portal Group Name: tpgroup_1
               Target Session ID: 2
                      Command ID: 20797
                  Initiator Name: iqn.1993-08.org.debian:01:fa752b8a5a3a
                 Initiator Alias: alias_1
             Initiator Session ID: 00:02:3d:01:00:00
                   Command Sub ID: 20797
                    Command State: Scsicdb_Waiting_STLayer
                     Command Type: Sequenced
```

Displays detailed information for active iSCSI commands in Vserver vs_1.

vserver iscsi connection show

Display active iSCSI connections

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command displays iSCSI connection information within a session. If you do not specify a connection, the command displays all information for all connections.

An active iSCSI session can contain one or multiple iSCSI connections. If an iSCSI connection has not completed the iSCSI login sequence, the iSCSI session might not contain iSCSI connections.

This command gives real-time status of connection activity. You can use the parameters header-digest-enabled and data-digest-enabled to troubleshoot performance problems.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Vserver

Use this parameter to display iSCSI connections that match the Vserver that you specify.

[-tpgroup <text>] - Target Portal Group

Use this parameter to display iSCSI connections that match the target portal group that you specify.

[-tsih <integer>] - Target Session ID

Use this parameter to display iSCSI connections that match the target session ID that you specify.

[-connection-id <integer>] - Connection ID

Use this parameter to display iSCSI connections that match the connection ID that you specify.

[-connection-state <iSCSI Connection State>] - Connection State

Use this parameter to display iSCSI connections that match the connection state you specify.

[-has-session {true|false}] - Connection Has session

Specifies if a session is established for a connection. If you enter this command using the parameter without a value, it is set to true, and the command displays all connections that have an established session. If you set this parameter to false, the command displays all connections that do not have established sessions.

[-lif <text>] - Logical interface

Use this parameter to display iSCSI connections that match the logical interface that you specify.

[-tpgroup-tag <integer>] - Target Portal Group Tag

Use this parameter to display iSCSI connections that use the target portal group tag that you specify.

[-local-address <text>] - Local IP Address

Use this parameter to display iSCSI connections that use the local IP address that you specify.

[-local-ip-port <integer>] - Local TCP Port

Use this parameter to display iSCSI connections that use the local TCP port that you specify.

[-authentication-method {CHAP|deny|none}] - Authentication Type

Use this parameter to display iSCSI connections that match the authentication type that you specify. CHAP requires password validation. Deny does not allow connections. None allows all connections.

[-data-digest-enabled {true|false}] - Data Digest Enabled

Specifies if data digest is enabled for a connection. If you enter this command using the parameter without a value, it is set to true, and the command displays all connections that support data digest. If you set this parameter to false, the command displays all connections that do not support data digest.

[-header-digest-enabled {true|false}] - Header Digest Enabled

Specifies if header digest is supported. If you enter this command using the parameter without a value, it is set to true, and the command shows all connections that support header digest. If you set this parameter to false, the command displays all connections that do not support header digest.

[-rcv-window-size <integer>] - TCP/IP Recv Size

Use this parameter to display iSCSI connections that match the specified negotiated size of the TCP/IP receive window in bytes.

[-initiator-mrdsl <integer>] - Initiator Max Recv Data Length

Use this parameter to display iSCSI connections that match the maximum length of message that the initiator can receive.

[-remote-address <text>] - Remote IP address

Use the parameter to display iSCSI connections that match the IP address of the initiator that you specify.

[-remote-ip-port <integer>] - Remote TCP Port

Use this parameter to display iSCSI connections that match the specified TCP port of initiator that you specify.

[-target-mrdsl <integer>] - Target Max Recv Data Length

Use this parameter to display iSCSI connections that match the maximum message size that a target can receive.

Examples

```
cluster1::> vserver iscsi connection show -vserver vs1
             Tpgroup              Conn  Local           Remote          TCP
Recv
Vserver      Name           TSIH  ID    Address         Address
Size
------------ ------------- ----- ----- --------------- ---------------
--------
vs1          vs1.iscsi          6     0 10.63.8.163     10.60.141.65
131400
vs1          vs1.iscsi          7     0 10.63.8.163     10.62.8.75
131400
2 entries were displayed.
```

Displays connection information on Vserver vs1.

vserver iscsi connection shutdown

Shut down a connection on a node

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

This command shuts down a specified iSCSI connection within a session. If you want to shut down all iSCSI connections in a session, use the vserver iscsi session shutdown command.

Parameters

`-vserver <Vserver Name>` - Vserver (privilege: advanced)

Specifies the Vserver.

`-tpgroup <text>` - Target Portal Group (privilege: advanced)

Specifies the target portal group that contains the connection you want to shut down.

`-tsih <integer>` - Target Session ID (privilege: advanced)

Specifies the target session ID that you want to shut down.

`-connection-id <integer>` - Connection ID (privilege: advanced)

Specifies the connection ID that you want to shut down.

Examples

```
cluster1::*> vserver iscsi connection shutdown -vserver vs_1 -tpgroup
tpgroup_1 -tsih 4 -connection-id 0
```

Forces the shutdown of an iSCSI connection with the connection ID of 0 on Vserver vs_1 in tpgroup tpgroup_1,

target session ID 4.

Related Links

- vserver iscsi session shutdown

vserver iscsi initiator show

Display iSCSI initiators currently connected

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command displays a list of active initiators currently connected to a specified Vserver.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Vserver

Use this parameter to display the active initiators that match the Vserver that you specify.

[-tpgroup <text>] - Target Portal Group

Use this parameter to display the active initiators that match the name of the target portal group that you specify.

[-tsih <integer>] - Target Session ID

Use this parameter to display the active initiators that match the target session ID you that specify.

[-initiator-name <text>] - Initiator Name

Use this parameter to display the active initiators that match the initiator name that you specify.

[-initiator-alias <text>] - Initiator Alias

Use this parameter to display the active initiators that match the alias name that you specify.

[-tpgroup-tag <integer>] - TPGroup Tag

Use this parameter to display the active initiators that match the target portal group tag that you specify.

[-isid <text>] - Initiator Session ID

Use this parameter to display the active initiators that match the initiator session ID that you specify.

[-igroup <text>,…] - Igroup Name

Use this parameter to display the active initiators that match the initiator group that you specify.

Examples

```
cluster1::> vserver iscsi initiator show -vserver vs_1
        Tpgroup       Initiator
Vserver Name     TSIH Name                   ISID              IGroup
------- -------- ---- -------------------- -----------------
-----------------
vs_1    vs_1.iscsi  6 iqn.1994-05.com.redhat:6ed6dfb0489e
                                            00:02:3d:03:00:00 -
vs_1    vs_1.iscsi  7 iqn.1993-08.org.debian:01:fa752b8a5a3a
                                            00:02:3d:01:00:00 igroup_1
2 entries were displayed.
```

Displays the active initiator information on Vserver vs_1.

vserver iscsi interface disable

Disable the specified interfaces for iSCSI service

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command disables the specified logical interfaces for an iSCSI service. Once disabled, all subsequent attempts to establish new iSCSI connections over the logical interface will fail.

Parameters

-vserver <Vserver Name> - Vserver

Specifies the Vserver.

{ -lif <lif-name>,... - Logical Interface

Specifies the logical interfaces on a Vserver you want to disable.

| -a, -all <true> - All }

Specifies that all logical interfaces on the Vserver are disabled.

[-f, -force <true>] - Force

When set to true, forces the termination of any active iSCSI sessions without prompting you for a confirmation.

Examples

```
cluster1::> vserver iscsi interface disable -vserver vs_1 -lif vs_1.iscsi
```

Disables the iscsi logical interface vs_1.iscsi on Vserver vs_1.

vserver iscsi interface enable

Enable the specified interfaces for iSCSI service

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command enables specified logical interfaces for iSCSI Vserver service. Once enabled, your system accepts new iSCSI connections and services iSCSI requests over the newly enabled logical interfaces.

Parameters

`-vserver <Vserver Name>` - Vserver

Specifies the Vserver.

{ `-lif <lif-name>,…` - Logical Interface

Specifies the logical interfaces on a Vserver that you want to enable.

| `-a, -all <true>` - All }

When set to true, all logical interfaces are enabled. If you use this parameter without a value, it is set to true, and the command enables all logical interfaces.

Examples

```
cluster1::> vserver iscsi interface enable -vserver vs_1 -lif vs_1.iscsi
```

Enables the iscsi logical interface vs_1.iscsi on Vserver vs_1.

vserver iscsi interface modify

Modify network interfaces used for iSCSI connectivity

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

The `vserver iscsi interface modify` command modifies the iSCSI specific configuration for an iSCSI LIF.

Parameters

`-vserver <Vserver Name>` - Vserver

Specifies the Vserver.

`-lif <lif-name>` - Logical Interface

Use this parameter to specify the logical interface on a Vserver that you want to modify.

[-sendtargets-fqdn <text>] - iSCSI Discovery SendTargets FQDN (privilege: advanced)

Use this parameter to specify the Fully Qualified Domain Name (FQDN) to return during an iSCSI Discovery SendTargets operation. To clear the FQDN, set this parameter to "". If unset, the IP address of the LIF is used in iSCSI SendTargets discovery. + This is not part of iSNS and will not affect the iSNS configuration.

Examples

The following example modifies the sendtargets-fqdn of the iSCSI LIF vs1_iscsi1 for Vserver vs1 to myhost.example.com.

```
cluster1::> vserver iscsi interface modify -vserver vs1 -lif vs1_iscsi1
-sendtargets_fqdn myhost.example.com
```

vserver iscsi interface show

Show network interfaces used for iSCSI connectivity

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command shows the iSCSI logical interfaces for a specified Vserver. If you do not specify any of the parameters, the command displays all of the interfaces on a Vserver.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Vserver

Use this parameter to display iSCSI logical interfaces that match the Vserver that you specify.

[-lif <lif-name>] - Logical Interface

Use this parameter to display iSCSI logical interfaces that that you specify.

[-status-admin {up|down}] - Administrative Status

Specifies the configured status of the logical interface. If you set this parameter to up, the command displays all iSCSI logical interfaces with the administrative status of up. If you set this parameter to down, the command displays all the iSCSI logical interfaces with the administrative status of down.

[-status-oper {up|down}] - Operational Status

Specifies the current status of the logical interface. If you set this parameter to up, the command displays all the iSCSI logical interfaces with the operational status of up. If you set this parameter to down, the command displays all the iSCSI logical interfaces with the operational status of down.

[-enabled {true|false}] - Enabled

Specifies if this logical unit is enabled for iSCSI service. If you enter this command without a parameter, its effective value is true, and the command displays all the enabled iSCSI logical interfaces.

[-address <IP Address>] - IP Address

Use this parameter to display iSCSI logical interfaces that match the IP address that you specify.

[-ip-port <integer>] - IP Port Number

Use this parameter to display iSCSI logical interfaces that match IP port number for the logical interface that you specify.

[-curr-node <nodename>] - Current Node

Use this parameter to display iSCSI logical interfaces that match current node that you specify.

[-curr-port {<netport>|<ifgrp>}] - Current Port

Use this parameter to display iSCSI logical interfaces that match specified current physical port that you specify.

[-is-home {true|false}] - Is Home

Specifies if the node hosting the logical interface is the initially configured node. If you use this command without using this parameter, it is set to true, and the command displays all iSCSI interfaces that are on the initially configured node.

[-tpgroup <text>] - TPGroup Name

Use this parameter to display iSCSI logical interfaces that match the target portal group name that you specify.

[-t, -tpgroup-tag <integer>] - TPGroup Tag

Use this parameter to display iSCSI logical interfaces that match the target portal group tag that you specify.

[-relative-port-id <integer>] - Relative Port ID

Use this parameter to display the iSCSI logical interface that matches the relative target port ID that you specify. The system assigns each logical interfaces and target portal group a relative target port ID that is Vserver unique. You cannot change this ID.

[-sendtargets-fqdn <text>] - iSCSI Discovery SendTargets FQDN (privilege: advanced)

Use this parameter to display the iSCSI logical interfaces that match the iSCSI Discovery SendTargets Fully Qualified Domain Name (FQDN) that you specify.

Examples

The following example displays information for logical interfaces on Vserver vs_1.

```
cluster1::> vserver iscsi interface show -vserver vs_1
           Logical         Status     IP              Curr        Curr
Vserver    Interface  TPGT Admin/Oper Address         Node        Port
Enabled
---------- ---------- ---- ---------- --------------- ----------- ----
-------
vs_1       vs_1.iscsi 1027   up/up    10.63.8.165     node1       e0c
true
vs_1       vs_1.iscsi2
                      1028   up/up    10.63.8.166     node1       e0c
true
2 entries were displayed.
```

The following example displays the logical interface vs_1.iscsi with the relative target port ID of 1.

```
cluster1::> vserver iscsi interface show -vserver vs_1 -relative-port-id 1
           Logical         Status     IP              Curr        Curr
Vserver    Interface  TPGT Admin/Oper Address         Node        Port
Enabled
---------- ---------- ---- ---------- --------------- ----------- ----
-------
vs_1       vs_1.iscsi 1027   up/up    10.63.8.165     node1       e0c
true
```

vserver iscsi interface accesslist add

Add the iSCSI LIFs to the accesslist of the specified initiator

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command adds network interfaces to an access list for a specified initiator. An access list ensures that an initiator only logs in with IP addresses associated with the interfaces defined in the access list.

You can restrict an initiator to certain network interfaces to improve performance and security. Access lists are useful where a particular initiator cannot access all of the network interfaces on a node.

Access list policies are based on the interface name. The accesslist rules are:

- If you disable the network interface for iSCSI through the vserver iscsi interface disable command, for example, the network interface is not accessible to any initiator regardless of any access lists in effect.
- If an initiator does not have an access list, that initiator can access any iSCSI-enabled network interface.
- If an initiator has an access list, that initiator can only login to network interfaces in its access list. Additionally, the initiator cannot discover any IP addresses that are not on this access list. If an initiator sends an iSCSI sendtargets request, the node responds with a list of IP addresses for iSCSI data logical

interfaces that are in its access list.

- If an initiator does not have an access list, you automatically create an access list when you issue the `vserver iscsi interface accesslist add` command.
- If you remove all the interfaces from the access list of an initiator with the vserver iscsi interface accesslist remove command, the accesslist is also deleted.
- Creating or modifying access list requires that initiator log out and log back in before changes take effect.

When you use the add or remove commands, the system warns you if an iSCSI session could be affected.

You will not affect any iSCSI sessions if you use the -a parameter when adding or removing all interfaces.

Parameters

`-vserver <Vserver Name>` - Vserver

Specifies the Vserver name.

`-initiator-name <text>` - Initiator Name

Specifies the initiator you want to add to the access list.

{ `-lif <lif-name>,…` - Logical Interface

Specifies the lif you want to add to an access list.

| `-a, -all <true>` - All }

If you use this parameter without a value, it is set to true, and the command adds all iSCSI data logical interfaces for a vserver to an initiator's accesslist. If the initiator does not have an accesslist, the system creates a new accesslist.

`[-f, -force <true>]` - Force

If you use this parameter without a value, it is set to true, and the command does not prompt you when an active iSCSI service or any active iSCSI data logical interfaces could be affected. If you do not use this parameter, the command prompts for confirmation if the iSCSI service is active or if any active data logical interfaces would be affected.

Examples

```
cluster1::> vserver iscsi interface accesslist add -vserver vs_1
-initiator-name iqn.1992-08.com.example:abcdefg -a
```

Adds the initiator iqn.1992-08.com.example:abcdefg on Vserver vs_1 for all iSCSI data logical interfaces in vs_1.

Related Links

- vserver iscsi interface disable
- vserver iscsi interface accesslist remove

vserver iscsi interface accesslist remove

Remove the iSCSI LIFs from the accesslist of the specified initiator

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command removes network interfaces from an access list for a specified initiator. The system removes the access list when the list is empty. When you remove a network interface from an initiator, this action could result in the shutdown of active sessions.

Parameters

`-vserver <Vserver Name>` - Vserver

Specifies the Vserver name.

`-initiator-name <text>` - Initiator Name

Specifies the initiator that you want to remove logical interfaces from.

{ `-lif <lif-name>,…` - Logical Interface

Specifies the logical interface you want to remove.

| `-a, -all <true>` - All }

If you use this parameter without a value, it is set to true, and the command removes all of the iSCSI data logical interfaces from an initiator's accesslist. If you remove all the network interfaces from an access list, the system removes the access list.

`[-f, -force <true>]` - Force

If you use this parameter without a value, it is set to true, and the command does not prompt you when an active iSCSI service or any active iSCSI data logical interfaces could be affected. If you do not use this parameter, the command prompts for confirmation if the iSCSI service is active or if any active data logical interfaces would be affected.

Examples

```
cluster1::> vserver iscsi interface accesslist remove -vserver vs_1
-initiator-name iqn.1992-08.com.example:abcdefg -a
```

Removes all the network interfaces from the access list for initiator iqn.1992-08.com.example:abcdefg on Vserver vs_1.

vserver iscsi interface accesslist show

Show accesslist of the initiators for iSCSI connectivity

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command displays an access list for an initiator. An access list is a list of logical interfaces that an initiator can use for iSCSI logins. The system records the access lists as part of the node configuration and preserves the access lists during reboots.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Vserver

Use this parameter to display the access lists that match the Vserver name that you specify.

[-initiator-name <text>] - Initiator Name

Use this parameter to display the access lists that match the initiator that you specify.

[-lif <lif-name>] - Logical Interface

Use this parameter to display the access lists that match the logical interface that you specify.

Examples

```
cluster1::> vserver iscsi interface accesslist show -vserver vs1
Vserver            Initiator Name                Logical Interface
------------------ ------------------------------
------------------------------
vs1                iqn.2010-01.com.example:aaaaa isw1
                                                 isw2
                   iqn.2010-01.com.example:aaabb isw1
                                                 isw2
4 entries were displayed.
```

Displays the access lists for vserver vs1.

vserver iscsi isns create

Configure the iSNS service for the Vserver

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command creates and starts an iSNS service with the IP address of the iSNS server.

A Vserver management LIF must exist before you can create an iSNS service. This LIF is used to communicate with the iSNS server. To create a Vserver management LIF, use the network interface create command, with `-role` *data* and `-data-protocol` *none*.

Parameters

`-vserver <Vserver Name>` - Vserver Name

Specifies the Vserver for the iSNS service that you want to create.

`-address <IP Address>` - iSNS Server IP Address

Specifies the IP address of the iSNS server. Both IPv4 and IPv6 address families are supported. The address family must be the same as that of the vserver management LIF.

A default route must exist for the specified vserver. To create a route, use the `network routing-groups route create` command. To view existing routes, use the `network routing-groups route show` command.

`[-status-admin {down|up}]` - Administrative Status

Specifies the administrative status of the iSNS service of a Vserver. If you set this parameter to up, the iSNS service starts for the Vserver and registers with the configured iSNS server. If you set this parameter to down, the Vserver loses its ability to register with the iSNS server and to be discovered by iSNS clients.

`[-force <true>]` - Force

`vserver iscsi isns create` fails if vserver management LIF is not configured. When you set this option to "true," you create an iSNS service on a Vserver even if the vserver does not have a vserver management LIF.

Examples

```
cluster1::> vserver iscsi isns create -vserver vs_1 -address 10.60.1.1
-status-admin up
```

Creates the iSNS service for Vserver vs_1 using the IPv4 address.

```
cluster1::> vserver iscsi isns create -vserver vs_1 -address
fd20:8b1e:b255:840b:a0df:565b:19b5:4d06 -status-admin up
```

Creates the iSNS service for Vserver vs_1 using the IPv6 address.

Related Links

- network interface create

vserver iscsi isns delete

Remove the iSNS service for the Vserver

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command deletes the iSNS service for the Vserver.

Parameters

`-vserver <Vserver Name>` - Vserver Name

Specifies the Vserver for the iSNS service that you want to delete.

Examples

```
cluster1::> vserver iscsi isns delete -vserver vs_1
```

Deletes the iSNS service for Vserver vs_1.

vserver iscsi isns modify

Modify the iSNS service for the Vserver

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command modifies the configuration of an iSNS service.

Modifications take effect immediately after you execute the command.

Parameters

`-vserver <Vserver Name>` - Vserver Name

Specifies the Vserver for the iSNS service that you want to modify.

`[-address <IP Address>]` - iSNS Server IP Address

Specifies the IP address of the iSNS server. Both IPv4 and IPv6 address families are supported. The address family must be the same as that of the vserver management LIF.

> A default route must exist for the specified vserver. To create a route, use the `network routing-groups route create` command. To view existing routes, use the `network routing-groups route show` command.

`[-status-admin {down|up}]` - Administrative Status

Specifies the administrative status of the iSNS service of a Vserver. If you set this parameter to up, the iSNS service starts for the Vserver, and registers with the configured iSNS server. If you set this parameter to down, the Vserver loses its ability to register with the iSNS server and to be discovered by iSNS clients.

[-force <true>] - Force

`vserver iscsi isns modify` fails to modify the iSNS server address if vserver management LIF is not configured. When you set this option to "true," you can modify the iSNS service on a Vserver even if the vserver does not have a vserver management LIF.

Examples

```
cluster1::> iscsi isns modify -vserver vs_1 -status-admin up
```

Modifies the status-admin of the iSNS service for Vserver vs_1 to up.

vserver iscsi isns show

Show iSNS service configuration

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

Shows the iSNS service configuration.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Vserver Name

Use this parameter to display the iSNS services that match the Vserver name that you specify.

[-address <IP Address>] - iSNS Server IP Address

Use this parameter to display the iSNS services that match the IP address of the iSNS server that you specify.

[-status-admin {down|up}] - Administrative Status

Use this parameter to display the iSNS services that match the configured status of the service that you specify.

[-entity-id <text>] - iSNS Server Entity Id

Use this parameter to display the iSNS services that match the configured iSNS server entity-id that you specify.

[-last-successful-update <MM/DD/YYYY HH:MM:SS>] - Last Successful Update

Use this parameter to display the iSNS services that match the time of the last successful attempt.

[-last-update-attempt <MM/DD/YYYY HH:MM:SS>] - Last Update Attempt

Use this parameter to display the iSNS services that match the time of the last update attempt.

[-last-update-result <isnsErrors>] - Last Update Result

Use this parameter to display the iSNS services that match the result of the last update attempt.

Examples

```
cluster1::> vserver iscsi isns show
Vserver    iSNS Server Entity Identifier   iSNS Server IP Address iSNS
Status
---------- ------------------------------ ----------------------
-----------
iscsi_vs   isns:00000044                  10.229.136.188         up
```

Displays the output of the show command for all Vservers in a cluster.

```
cluster1::> vserver iscsi isns show -instance
          Vserver Name: vs1
iSNS Server IP Address: 10.72.19.11
 Administrative Status: up
 iSNS Server Entity Id: isns.0000001c
Last Successful Update: 11/12/2011 10:18:45
   Last Update Attempt: 11/12/2011 10:18:45
    Last Update Result: iSNS_Ok

Vserver Name: vs2
iSNS Server IP Address: 10.72.16.13
 Administrative Status: up
 iSNS Server Entity Id: isns.0000001b
Last Successful Update: 11/12/2011 13:38:05
   Last Update Attempt: 11/12/2011 13:38:05
    Last Update Result: iSNS_Ok


2 entries were displayed.
```

Displays the details for all Vservers in a cluster.

vserver iscsi isns start

Starts the iSNS service

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

Starts the iSNS service. Once you start the iSNS service, the Vserver automatically register with the iSNS server.

Parameters

-vserver <Vserver Name> - Vserver Name

Specifies the Vserver for the iSNS service that you want to start.

Examples

```
cluster1::> vserver iscsi isns start -vserver vs_1
```

Starts the iSNS service for Vserver vs_1.

vserver iscsi isns stop

Stops the iSNS service

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

Stops the iSNS service. Once you stop the iSNS service, the Vserver loses the ability to register with the iSNS server and to be discovered by iSNS clients.

Parameters

-vserver <Vserver Name> - Vserver Name

Specifies the Vserver for the iSNS service that you want to stop.

Examples

```
cluster1::> vserver iscsi isns stop -vserver vs_1
```

Stops the iSNS service for Vserver vs_1.

vserver iscsi isns update

Force update of registered iSNS information

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

Forces an update of the registration information with the iSNS server. Normally, the system checks for iSNS

configuration changes on the Vserver every few minutes and automatically sends updates to the iSNS server.

Parameters

`-vserver <Vserver Name>` - Vserver Name

Specifies the Vserver for the iSNS service that you want to update.

Examples

```
cluster1::> vserver iscsi isns update -vserver vs_1
```

Updates the iSNS server registration for Vserver vs_1.

vserver iscsi security add-initator-address-ranges

Add IP Address Ranges

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

Add IP address ranges to an existing iSCSI security entry

Parameters

`-vserver <Vserver Name>` - Vserver

Specifies the Vserver.

`-i, -initiator-name <text>` - Initiator Name

Specifies the initiator.

`-initiator-address-ranges {<ipaddr>|<ipaddr>-<ipaddr>}` - Initiator IP Address Ranges

Specifies one or more initiator source IP address range. The IPv4 or IPv6 address range contains a start address and an end address. The start and end addresses themselves are included in the range.

An example of a valid IPv4 address range is: '192.168.1.100-192.168.1.150'.

An example of a valid IPv6 address range is: '2001:db8::1000:1-2001:db8::1000:50'.

Examples

```
cluster1::> vserver iscsi security add-initator-address-range
-vserver vs1 -initiator-name iqn.1993-08.com.example:01:e3f87c7cf2e4
-initiator-address-range 192.168.2.1-192.168.2.255
```

Adds the IP address range 192.168.2.1-192.168.2.255 to initiator iqn.1993-08.com.example:01:e3f87c7cf2e4 for vserver vs1.

vserver iscsi security create

Create an iSCSI authentication configuration for an initiator

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command configures the security method for an iSCSI initiator on a Vserver. The outbound CHAP password and user name are optional. If you want mutual authentication, you need to configure both inbound and outbound CHAP passwords and user names.

You cannot use the same password for inbound and outbound settings.

Parameters

`-vserver <Vserver Name>` - Vserver

Specifies the Vserver.

`-i, -initiator-name <text>` - Initiator Name

Specifies the initiator that you want to create a security method for. You can use either an iqn such as iqn.1995-08.com.example:string or eui such as eui.0123456789abcdef for the initiator.

`-s, -auth-type {CHAP|deny|none}` - Authentication Type

Specifies the authentication type:

- CHAP - Authenticates using a CHAP user name and password.
- none - The initiator can access the Vserver without authentication.
- deny - The initiator cannot access the Vserver.

`[-n, -user-name <text>]` - Inbound CHAP User Name

Specifies the inbound CHAP user name. CHAP user names can be one to 128 bytes. A null user name is not allowed. If provided, you will be prompted to provide the corresponding inbound CHAP password.

`[-m, -outbound-user-name <text>]` - Outbound CHAP User Name

Specifies the outbound CHAP user name. CHAP user names can be one to 128 bytes. If provided, you will be prompted to enter the corresponding outbound CHAP password.

`[-initiator-address-ranges {<ipaddr>|<ipaddr>-<ipaddr>}]` - Initiator IP Address Ranges

Specifies one or more initiator source IP address ranges. If this list is empty, the initiator is allowed to log in from any IP address. The IPv4 or IPv6 address range contains a start address and an end address. The start and end addresses themselves are included in the range.

An example of a valid IPv4 address range is: '192.168.1.100-192.168.1.150'.

An example of a valid IPv6 address range is: '2001:db8::1000:1-2001:db8::1000:50'.

Examples

```
cluster1::> vserver iscsi security create -initiator
eui.0123456789abcdef -auth-type CHAP -user-name bob -outbound-user-name
bob2

Password: {enter password}

Outbound Password: {enter password}
```

Creates authentication method chap for initiator eui.0123456789abcdef with inbound and outbound usernames and passwords.

```
cluster1::> vserver iscsi security create -vserver vs_1
-initiator-name iqn.1995-08.com.example:e3f87c7cf2e4 -auth-type none
-initiator-address-ranges 192.168.1.1-192.168.1.255
```

Creates authentication method for initiator iqn.1993-08.com.example:01:e3f87c7cf2e4 with IP address validation only.

vserver iscsi security default

Configure the default authentication settings

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command defines a default iSCSI authentication method for your Vserver. If you do not configure the initiator to use a user-defined authentication method, the system assigns the default authentication method automatically to the initiator. Use the vserver iscsi security create command if you want to configure a user-defined authentication method.

The outbound CHAP user name and password are optional. If you want a bi-directional handshake, provide the outbound user name and you will be prompted for the corresponding password.

You cannot use the same password for inbound and outbound settings.

Parameters

`-vserver <Vserver Name>` - Vserver

Specifies the Vserver.

`-s, -auth-type {CHAP|deny|none}` - Authentication Method

Specifies the authentication type:

- CHAP - Authenticates using a CHAP user name and password.
- none - The initiator can access the Vserver without authentication.

- deny - The initiator cannot access the Vserver.

[-n, -user-name <text>] - Inbound CHAP User Name

Specifies the inbound CHAP user name. CHAP user names can be one to 128 bytes. A null user name is not allowed. If provided, you will be prompted to provide the corresponding inbound CHAP password.

{ [-m, -outbound-user-name <text>] - Outbound CHAP User Name

Specifies the outbound CHAP user name. CHAP user names can be one to 128 bytes. If provided, you will be prompted to enter the corresponding outbound CHAP password.

| [-clear-outbound <true>] - Clear Outbound CHAP Parameters }

Removes the outbound user name and the outbound password information from the default authentication method. After you clear the outbound information, you no longer have a bi-directional handshake.

Examples

```
cluster1::> vserver iscsi security default -vserver vs1 -security chap
-user-name bob -outbound-user-name bob_out

Password:

Outbound Password:
```

Sets the default authentication method to CHAP with inbound and outbound user names and passwords.

Related Links

- vserver iscsi security create

vserver iscsi security delete

Delete the iSCSI authentication configuration for an initiator

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command removes the security settings for this initiator. The default authentication setting now applies to this initiator.

Parameters

-vserver <Vserver Name> - Vserver

Specifies the Vserver.

-i, -initiator-name <text> - Initiator Name

Specifies the initiator that you want to remove the authentication setting from.

Examples

```
cluster1::> vserver iscsi security delete -vserver vs1 -initiator
iqn.1992-08.com.example:abcdefg
```

Deletes initiator iqn.1992-08.com.example:abcdefg on Vserver vs1 from the authentication setting. The default authentication now applies to this initiator.

vserver iscsi security modify

Modify the iSCSI authentication configuration for an initiator

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The command modifies an existing authentication method for an initiator. To delete the authentication setting for an initiator, use the vserver iscsi security delete command.

The outbound CHAP password and user name are optional. If you want a bi-directional handshake, you need to configure both inbound and outbound CHAP passwords and user names.

You do not need to know the inbound or outbound passwords to change them.

Parameters

`-vserver <Vserver Name>` - Vserver

Specifies the Vserver.

`-i, -initiator-name <text>` - Initiator Name

Specifies the initiator name that you want to modify the existing authentication method.

`[-s, -auth-type {CHAP|deny|none}]` - Authentication Type

Specifies the authentication type:

- CHAP - Authenticates using a CHAP user name and password.
- none - The initiator can access the Vserver without authentication.
- deny - The initiator cannot access the Vserver.

`[-n, -user-name <text>]` - Inbound CHAP User Name

Specifies the inbound CHAP user name. CHAP user names can be one to 128 bytes. A null user name is not allowed. If provided, you will be prompted to provide the corresponding inbound CHAP password.

`{ [-m, -outbound-user-name <text>]` - Outbound CHAP User Name

Specifies the outbound CHAP user name. CHAP user names can be one to 128 bytes. If provided, you will be prompted to enter the corresponding outbound CHAP password.

| [-clear-outbound <true>] - Clear Outbound CHAP Parameters }

Removes the outbound user name and the outbound password information from the authentication method. After you clear the outbound information, you no longer have a bi-directional handshake.

Examples

```
cluster1::> vserver iscsi security modify -vserver vs_1 -initiator
iqn.1992-08.com.example:abcdefg -auth-type chap -user-name bob -outbound
-user-name bob_out

Password:

Outbound Password:
```

Changes user names and passwords for initiator iqn.1992-08.com.example:abcdefg on Vserver vs_1.

Related Links

- vserver iscsi security delete

vserver iscsi security prepare-to-downgrade

Prepares the system for downgrade

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

This command prepares the cluster for a downgrade to an earlier version of Data ONTAP. Before using this command verify that all security entries do not have any initiator address ranges defined. This may be done by running the command vserver iscsi security show *address-ranges*

Examples

```
cluster1::> vserver iscsi security prepare-to-downgrade
```

The above example will verify that the cluster is able to downgrade to a prior release of Data ONTAP.

Related Links

- vserver iscsi security show

vserver iscsi security remove-initator-address-ranges

Remove an IP Address Range

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

Remove IP address ranges to an existing iSCSI security entry

Parameters

`-vserver <Vserver Name>` - Vserver

Specifies the Vserver.

`-i, -initiator-name <text>` - Initiator Name

Specifies the initiator.

`-initiator-address-ranges {<ipaddr>|<ipaddr>-<ipaddr>}` - Initiator IP Address Ranges

Specifies one or more initiator source IP address range. The IPv4 or IPv6 address range contains a start address and an end address. The start and end addresses themselves are included in the range.

An example of a valid IPv4 address range is: '192.168.1.100-192.168.1.150'.

An example of a valid IPv6 address range is: '2001:db8::1000:1-2001:db8::1000:50'.

Examples

```
netapp-clus-1::> vserver iscsi security remove-initator-address-range
-vserver vs1 -initiator-name iqn.1993-08.com.example:01:e3f87c7cf2e4
-initiator-address-range 192.168.2.1-192.168.2.255
```

Removes the IP address range 192.168.2.1-192.168.2.255 to the initiator iqn.1993-08.com.example:01:e3f87c7cf2e4 for vserver vs1.

vserver iscsi security show

Show the current iSCSI authentication configuration

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command displays the default authentication and all initiator-specific authentication information. Data ONTAP authentication overrides all other service authentication methods.

Parameters

{ `[-fields <fieldname>,…]`

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-address-masks]

Display the list of IP Address ranges in CIDR notation that each initiator is allowed to originate from. If this list is empty, the initiator is allowed to log in from any IP address. The IPv4 or IPv6 address range contains a start address and an end address. The start and end addresses themselves are included in the range.

| [-address-ranges]

Display the list of IP Address ranges that each initiator is allowed to originate from. If this list is empty, the initiator is allowed to log in from any IP address. The IPv4 or IPv6 address range contains a start address and an end address. The start and end addresses themselves are included in the range.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Vserver

Use this parameter to display authentication information that matches the Vserver name that you specify.

[-i, -initiator-name <text>] - Initiator Name

Use this parameter to display authentication information that matches the initiator that you specify.

[-s, -auth-type {CHAP|deny|none}] - Authentication Type

Use this parameter to display authentication information that matches the authentication type that you specify.

[-n, -user-name <text>] - Inbound CHAP User Name

Use this parameter to display authentication information that matches the inbound CHAP user name that you specify.

[-m, -outbound-user-name <text>] - Outbound CHAP User Name

Use this parameter to display authentication information that matches the outbound CHAP user name that you specify.

[-auth-chap-policy <local>] - Authentication CHAP Policy

Use this parameter to display authentication information that matches the authentication CHAP policy that you specify.

[-initiator-address-ranges {<ipaddr>|<ipaddr>-<ipaddr>}] - Initiator IP Address Ranges

Use this parameter to display authentication information that matches the initiator address range that you specify. If this list is empty, the initiator is allowed to log in from any IP address. The IPv4 or IPv6 address range contains a start address and an end address. The start and end addresses themselves are included in the range.

An example of a valid IPv4 address range is: '192.168.1.100-192.168.1.150'.

An example of a valid IPv6 address range is: '2001:db8::1000:1-2001:db8::1000:50'.

[-initiator-address-masks <IP Address/Mask>,…] - Initiator IP Address Masks

Use this parameter to display authentication information that matches the initiator address masks that you specify. If this list is empty, the initiator is allowed to log in from any IP address. The IPv4 or IPv6 address range contains a start address and an end address. The start and end addresses themselves are included in the range.

An example of a valid IPv4 address range in CIDR notation is: 192.168.1.3/32.

An example of a valid IPv6 address range in CIDR notation is: 2001:db8::1000:1/128.

Examples

```
cluster1::> vserver iscsi security show -vserver vs1
                                  Auth   Auth CHAP Inbound CHAP  Outbound
CHAP
Vserver    Initiator Name         Type   Policy    User Name     User Name
---------- ---------------------- ------ --------- -------------
-------------
vs1        default                none   -         -             -
           iqn.2010-12.com.example:abcdefg
                                  CHAP   local     bob           bob2
2 entries were displayed.
```

Displays the authentication information for Vserver vs1.

```
cluster1::> vserver iscsi security show -address-ranges -vserver vs1

Vserver    Initiator Name         Initiator Address Ranges
---------- ----------------------
-------------------------------------------
vs1        iqn.2010-12.com.example:abcdefg
           iqn.2010-12.com.example:hijklmn
                                  192.168.1.100-192.168.1.150
                                  2001:db8::1000:1-2001:db8::1000:50

2 entries were displayed.
```

Displays the initiator and their valid address ranges for Vserver vs1.

```
cluster1::> vserver iscsi security show -address-masks -vserver vs1

Vserver    Initiator Name          Initiator Address Ranges
---------- ----------------------
-------------------------------------------
vs1        iqn.2010-12.com.example:abcdefg
     iqn.2010-12.com.example:hijklmn
          192.168.1.100/30
          192.168.1.104/29
          192.168.1.112/28
          192.168.1.128/28
          192.168.1.144/30
          192.168.1.148/31
          192.168.1.150/32
          2001:db8::1000:1/128
          2001:db8::1000:2/127
          2001:db8::1000:4/126
          2001:db8::1000:8/125
          2001:db8::1000:10/124
          2001:db8::1000:20/123
          2001:db8::1000:40/124
          2001:db8::1000:50/128
2 entries were displayed.
```

Displays the initiator and their valid address ranges for Vserver vs1.

vserver iscsi session show

Display iSCSI sessions

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command displays iSCSI session information. If you do not specify the target session ID (TSIH), the command displays all session information for the specified Vserver. If a Vserver is not specified, the command displays all session information in the cluster. Use the vserver iscsi connection show command to display connection information. Use the vserver iscsi session parameter show command to show the parameters used when creating the session.

You can use session information for troubleshooting performance problems.

An iSCSI session can have one or multiple connections. Typically a session has at least one connection.

Most of the parameters are read-only. However, some parameters can be modified with the vserver iscsi modify command.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Vserver

Use this parameter to display iSCSI session information that matches the Vserver name that you specify.

[-tpgroup <text>] - Target Portal Group

Use this parameter to display iSCSI session information that matches the target portal group name that you specify.

[-tsih <integer>] - Target Session ID

Use this parameter to display iSCSI session information that matches the target session ID that you specify.

[-max-ios-per-session <integer>] - Max Commands per Session

Use this parameter to display iSCSI session information that matches the maximum commands per session count you specify.

[-data-pdu-in-order {true|false}] - Data PDU in Order

Specifies if the data PDUs are in sequence order. If you enter this command without using this parameter, it is set to true, and the command displays all session information that supports PDUs in order. If you provide a false value, the command displays all session information that does not support PDUs in order.

[-data-sequence-in-order {true|false}] - Data Sequence in Order

Specifies if the data is in sequence order. If you enter this command without using this parameter, it is set to true, and the command displays all session information where data sequence is supported. If you provide a false value, the command displays all session information that does not support data sequence.

[-default-time-to-retain <integer>] - Default Time to Retain

Use this parameter to display session information that matches the retain time that you specify. This value specifies the amount of time before active reassignment is possible after an unexpected connection termination or a connection reset. A value of 0 means the connection task state is immediately discarded by the target.

[-default-time-to-wait <integer>] - Default Time to Wait

Use this parameter to display session information that matches the logout or active task assignment wait time that you specify. Wait time refers to the amount of time before attempting an explicit or implicit logout or active task assignment after an unexpected connection termination or connection reset.

[-error-recovery-level <integer>] - Error Recovery Level

Use this command to display session information that matches the error recovery level that you specify.

[-first-burst-length <integer>] - First Burst Length

Use this parameter to display session information that matches the first burst length that you specify. First burst length is the maximum amount of unsolicited data in bytes that can be sent during the execution of a

single iSCSI packet. First burst length covers the total amount of immediate data and the unsolicited data-out PDU. The first burst length must not exceed the maximum burst length.

[-immediate-data-enabled {true|false}] - Immediate Data

Specifies if immediate data is supported. When immediate data is supported, the initiator can send immediate data. If you enter this command using the parameter without a value, it is set to true, and the command displays all session information that supports immediate data. If you provide a false value, the command displays all session information that does not support immediate data.

[-initiator-alias <text>] - Initiator Alias

Use this parameter to display iSCSI session information that matches the alias name of the initiator that you specify.

[-initial-r2t-enabled {true|false}] - Initial R2T Enabled

Specifies if the initiator supports Initial Ready to Transfer (R2T). R2T is the mechanism that allows the target to request the initiator for output data. If you enter this command using the parameter without a value, it is set to true, and the command displays all session information that supports initial R2T data. If you provide a false value, the command displays all session information that does not support initial R2T data.

[-initiator-name <text>] - Initiator Name

Use this parameter to display the iSCSI session information that matches the initiator name that you specify.

[-isid <text>] - Initiator Session ID

Use this parameter to display iSCSI session information that matches the initiator session ID that you specify.

[-max-burst-length <integer>] - Max Burst Length for Session

Use this parameter to display iSCSI session information that matches the maximum burst length that you specify. Maximum burst length is the maximum iSCSI data payload in bytes for a data-in or solicited data-out sequence.

[-max-connections <integer>] - Max Connections for Session

Use this parameter to display iSCSI session information that matches the maximum number of connections that you specify.

[-max-outstanding-r2t <integer>] - Max Outstanding R2T for Session

Use this parameter to display iSCSI session information that matches the maximum number of outstanding R2T per task that you specify.

[-session-type <iSCSI Session Type>] - Session Type

Use this parameter to display iSCSI session information that matches the session type that you specify.

[-tpgroup-tag <integer>] - Target Portal Group Tag

Use this parameter to display iSCSI session information that matches the target portal group tag that you specify.

[-connection-ids <integer>,…] - Active Connection IDs

Use this parameter to display iSCSI session information that matches the active connection IDs that you specify.

Examples

```
cluster1::> vserver iscsi session show -vserver vs_1
          Tpgroup        Initiator                        Initiator
Vserver   Name    TSIH   Name                   ISID      Alias
--------- ------- ------ ---------------------- ---------
------------------------
vs_1      tpgroup_1
                  2      iqn.1993-08.org.debian:01:fa752b8a5a3a
                                                00:02:3d:01:00:00
                                                          initiator-alias
Displays session information for all sessions on Vserver vs_1.
```

Related Links

- vserver iscsi connection show
- vserver iscsi session parameter show
- vserver iscsi modify

vserver iscsi session shutdown

Shut down a session on a node

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

This command forces a shutdown of all connections in a session. If you want to shut down a single connection in a session, use the vserver iscsi connection shutdown command.

Parameters

-vserver <Vserver Name> - Vserver (privilege: advanced)

Specifies the Vserver.

-tpgroup <text> - Target Portal Group (privilege: advanced)

Specifies the target portal group that contains the session you want to shutdown.

-tsih <integer> - Target Session ID (privilege: advanced)

Specifies the target session ID that you want to shut down.

Examples

```
cluster1::*> vserver iscsi session shutdown -vserver vs_1 -tpgroup
tpgroup_1 -tsih 2
```

Forces a session shutdown for target session ID 2 in tpgroup_1 in Vserver vs_1 .

Related Links

- vserver iscsi connection shutdown

vserver iscsi session parameter show

Display the parameters used to establish an iSCSI session

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command displays session parameter information. This command is intended for troubleshooting performance problems.

Most of the parameters are read-only. However, some parameters can be modified with the vserver iscsi modify command.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Vserver

Use this parameter to display session information that matches the Vserver name that you specify.

[-tpgroup <text>] - Target Portal Group

Use this parameter to display session information that matches the target portal group name that you specify.

[-tsih <integer>] - Target Session ID

Use this parameter to display session information that matches the target session ID that you specify.

[-cmd-window-size <integer>] - Max Commands per Session

Use this parameter to display session information that matches the command window size that you specify.

[-data-pdu-in-order {true|false}] - Data PDU in Order

Use this parameter to display session information with the value of the Protocol Data Units (PDU) in order flag you specify. This parameter indicates if the data within a sequence can be in any order or must be in sequence. If you enter this command without using this parameter, it is set to true, and the command displays all session information that supports PDUs in order. If you provide a false value, the command displays all session information that does not support PDUs in order.

[-data-sequence-in-order {true|false}] - Data Sequence in Order

Use this parameter to display session information with the value of the data sequence in order flag that you specify. If you enter this command without using this parameter, it is set to true, and the command displays all session information that supports data sequence. If you set the values to false, the command displays all session information that does not support data sequence.

[-default-time-to-retain <integer>] - Default Time to Retain

Use this parameter to display session information that matches the retain time that you specify. This value specifies the amount of time before active reassignment is possible after an unexpected connection termination or a connection reset. A value of 0 means the connection task state is immediately discarded by the target.

[-default-time-to-wait <integer>] - Default Time to Wait

Use this parameter to display session information that matches the logout or active task assignment wait time that you specify. Wait time refers to the amount of time before attempting an explicit or implicit logout or active task assignment after an unexpected connection termination or connection reset.

[-error-recovery-level <integer>] - Error Recovery Level

Use this command to display session information that matches the error recovery level that you specify.

[-first-burst-length <integer>] - First Burst Length

Use this parameter to display session information that matches the first burst length that you specify. First burst length is the maximum amount of unsolicited data in bytes that can be sent during the execution of a single iSCSI packet. First burst length covers the total amount of immediate data and the unsolicited data-out PDU. The first burst length must not exceed the maximum burst length.

[-immediate-data-enabled {true|false}] - Immediate Data

Use this parameter to display session information with the value of the immediate data-enabled flag that you specify. If you enter this command without using this parameter, it is set to true, and the command displays all session information that supports immediate data. If you set the value to false, the command displays all session information that does not support immediate data.

[-initial-r2t-enabled {true|false}] - Initial R2T Enabled

Use this parameter to display session information with the value of the R2T data-enabled flag that you specify. If you enter this command without using this parameter, it is set to true, and the command displays all session information that supports R2T data. If you set the value to false, the command displays all session information that does not support R2T data.

[-initiator-alias <text>] - Initiator Alias

Use this parameter to display iSCSI session information that matches the initiator alias name you specify.

[-initiator-name <text>] - Initiator Name

Use this parameter to display iSCSI session information that matches the initiator name you specify.

[-isid <text>] - Initiator Session ID

Use this parameter to display iSCSI session information that matches the initiator session identifier you specify.

[-max-burst-length <integer>] - Max Burst Length for Session

Use this parameter to display iSCSI session information that matches the maximum burst length that you specify. Maximum burst length is the maximum iSCSI data payload in bytes for a data-in or solicited data-

out sequence.

[-max-connections <integer>] - Max Connections for Session

Use this parameter to display iSCSI session information that matches the maximum number of connections that you specify.

[-max-outstanding-r2t <integer>] - Max Outstanding R2T for Session

Use this parameter to display iSCSI session information that matches the maximum number of outstanding R2T per task that you specify.

[-session-type <iSCSI Session Type>] - Session Type

Use this parameter to display iSCSI session information that matches the session type you specify.

[-tpgroup-tag <integer>] - Target Portal Group Tag

Use this parameter to display iSCSI session information that matches the target portal group tag you specify.

[-initiator-mrdsl <integer>,…] - Initiator Max Recv Data Len

Use this parameter to display iSCSI session information that matches the initiator maximum receivable data segment length you specify. An iSCSI initiator declares the maximum data segment length in bytes it can receive in an iSCSI PDU during the iSCSI login phase.

[-target-mrdsl <integer>,…] - Target Max Recv Data Len

Use this parameter to display iSCSI session information that matches the target maximum receivable data segment length you specify. An iSCSI target declares the maximum data segment length in bytes it can receive in an iSCSI PDU during the iSCSI login phase.

Examples

```
cluster1::> iscsi session parameter show -vserver vs_1
        Tpgroup      Max  Data PDU Data Seq Time 2 Time 2 Error   Imm
Initial
Vserver Name    TSIH Conn In Order In Order Retain Wait   Rec Lvl Data
R2T
------- ------- ---- ---- -------- -------- ------ ------ ------- -----
-------
vs_1    vs_1.iscsi 6    1 true     true          0      2       0 true
false
vs_1    vs_1.iscsi 7    1 true     true          0      2       0 true
false
2 entries were displayed.
```

Lists iSCSI session parameters for Vserver vs_1.

Related Links

- vserver iscsi modify

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.