Table of Contents

iSCSI service management .............................................................. 1
iSCSI service management .............................................................. 1
How iSCSI authentication works ......................................................... 1
iSCSI initiator security management ..................................................... 2
iSCSI endpoint isolation ................................................................. 2
What CHAP authentication is ............................................................. 2
How using iSCSI interface access lists to limit initiator interfaces can increase performance and security ........................................ 3
iSNS server registration requirement ................................................ 3
You can manage the availability of the iSCSI service on the iSCSI logical interfaces of the storage virtual machine (SVM) by using the `vserver iscsi interface enable` or `vserver iscsi interface disable` commands.

By default, the iSCSI service is enabled on all iSCSI logical interfaces.

**How iSCSI is implemented on the host**

iSCSI can be implemented on the host using hardware or software.

You can implement iSCSI in one of the following ways:

- Using Initiator software that uses the host's standard Ethernet interfaces.
- Through an iSCSI host bus adapter (HBA): An iSCSI HBA appears to the host operating system as a SCSI disk adapter with local disks.
- Using a TCP Offload Engine (TOE) adapter that offloads TCP/IP processing.

The iSCSI protocol processing is still performed by host software.

**How iSCSI authentication works**

During the initial stage of an iSCSI session, the initiator sends a login request to the storage system to begin an iSCSI session. The storage system then either permits or denies the login request, or determine that a login is not required.

iSCSI authentication methods are:

- Challenge Handshake Authentication Protocol (CHAP)--The initiator logs in using a CHAP user name and password.

You can specify a CHAP password or generate a hexadecimal secret password. There are two types of CHAP user names and passwords:

  - Inbound—The storage system authenticates the initiator.

    Inbound settings are required if you are using CHAP authentication.

  - Outbound—This is an optional setting to enable the initiator to authenticate the storage system.

    You can use outbound settings only if you define an inbound user name and password on the storage system.

- deny—The initiator is denied access to the storage system.

- none—The storage system does not require authentication for the initiator.

You can define the list of initiators and their authentication methods. You can also define a default
authentication method that applies to initiators that are not on this list.

**Related information**

Windows Multipathing Options with Data ONTAP: Fibre Channel and iSCSI

### iSCSI initiator security management

ONTAP provides a number of features for managing security for iSCSI initiators. You can define a list of iSCSI initiators and the authentication method for each, display the initiators and their associated authentication methods in the authentication list, add and remove initiators from the authentication list, and define the default iSCSI initiator authentication method for initiators not in the list.

### iSCSI endpoint isolation

Beginning with ONTAP 9.1 existing iSCSI security commands were enhanced to accept an IP address range, or multiple IP addresses.

All iSCSI initiators must provide origination IP addresses when establishing a session or connection with a target. This new functionality prevents an initiator from logging into the cluster if the origination IP address is unsupported or unknown, providing a unique identification scheme. Any initiator originating from an unsupported or unknown IP address will have their login rejected at the iSCSI session layer, preventing the initiator from accessing any LUN or volume within the cluster.

Implement this new functionality with two new commands to help manage pre-existing entries.

**Add initiator address range**

Improve iSCSI initiator security management by adding an IP address range, or multiple IP addresses with the `vserver iscsi security add-initiator-address-range` command.

```
cluster1::> vserver iscsi security add-initiator-address-range
```

**Remove initiator address range**

Remove an IP address range, or multiple IP addresses, with the `vserver iscsi security remove-initiator-address-range` command.

```
cluster1::> vserver iscsi security remove-initiator-address-range
```

### What CHAP authentication is

The Challenge Handshake Authentication Protocol (CHAP) enables authenticated communication between iSCSI initiators and targets. When you use CHAP authentication, you define CHAP user names and passwords on both the initiator and the storage system.

During the initial stage of an iSCSI session, the initiator sends a login request to the storage system to begin the session. The login request includes the initiator’s CHAP user name and CHAP algorithm. The storage
system responds with a CHAP challenge. The initiator provides a CHAP response. The storage system verifies
the response and authenticates the initiator. The CHAP password is used to compute the response.

Guidelines for using CHAP authentication

You should follow certain guidelines when using CHAP authentication.

• If you define an inbound user name and password on the storage system, you must use the same user
  name and password for outbound CHAP settings on the initiator. If you also define an outbound user name
  and password on the storage system to enable bidirectional authentication, you must use the same user
  name and password for inbound CHAP settings on the initiator.

• You cannot use the same user name and password for inbound and outbound settings on the storage
  system.

• CHAP user names can be 1 to 128 bytes.
  
  A null user name is not allowed.

• CHAP passwords (secrets) can be 1 to 512 bytes.
  
  Passwords can be hexadecimal values or strings. For hexadecimal values, you should enter the value with
  a prefix of “0x” or “0X”. A null password is not allowed.

• For additional restrictions, you should see the initiator’s documentation.

  For example, the Microsoft iSCSI software initiator requires both the initiator and target CHAP passwords
  to be at least 12 bytes if IPsec encryption is not being used. The maximum password length is 16 bytes
  regardless of whether IPsec is used.

How using iSCSI interface access lists to limit initiator
interfaces can increase performance and security

iSCSI interface access lists can be used to limit the number of LIFs in an SVM that an
initiator can access, thereby increasing performance and security.

When an initiator begins a discovery session using an iSCSI SendTargets command, it receives the IP
addresses associated with the LIF (network interface) that is in the access list. By default, all initiators have
access to all iSCSI LIFs in the SVM. You can use the access list to restrict the number of LIFs in an SVM that
an initiator has access to.

iSNS server registration requirement

What iSNS is

The Internet Storage Name Service (iSNS) is a protocol that enables automated
discovery and management of iSCSI devices on a TCP/IP storage network. An iSNS
server maintains information about active iSCSI devices on the network, including their IP
addresses, iSCSI node names IQN’s, and portal groups.

You can obtain an iSNS server from a third-party vendor. If you have an iSNS server on your network
configured and enabled for use by the initiator and target, you can use the management LIF for a storage
virtual machine (SVM) to register all the iSCSI LIFs for that SVM on the iSNS server. After the registration is complete, the iSCSI initiator can query the iSNS server to discover all the LIFs for that particular SVM.

If you decide to use an iSNS service, you must ensure that your storage virtual machines (SVMs) are properly registered with an Internet Storage Name Service (iSNS) server.

If you do not have an iSNS server on your network, you must manually configure each target to be visible to the host.

**What an iSNS server does**

An iSNS server uses the Internet Storage Name Service (iSNS) protocol to maintain information about active iSCSI devices on the network, including their IP addresses, iSCSI node names (IQNs), and portal groups.

The iSNS protocol enables automated discovery and management of iSCSI devices on an IP storage network. An iSCSI initiator can query the iSNS server to discover iSCSI target devices.

NetApp does not supply or resell iSNS servers. You can obtain these servers from a vendor supported by NetApp.

**How SVMs interact with an iSNS server**

The iSNS server communicates with each storage virtual machine (SVM) through the SVM management LIF. The management LIF registers all iSCSI target node name, alias, and portal information with the iSNS service for a specific SVM.

In the following example, SVM VS1 uses the SVM management LIF vs1_mgmt_lif to register with the iSNS server. During iSNS registration, an SVM sends all the iSCSI LIFs through the SVM management LIF to the iSNS Server. After the iSNS registration is complete, the iSNS server has a list of all the LIFs serving iSCSI in VS1. If a cluster contains multiple SVMs, each SVM must register individually with the iSNS server to use the iSNS service.
In the next example, after the iSNS server completes the registration with the target, Host A can discover all the LIFs for VS1 through the iSNS server as indicated in step 1. After Host A completes the discovery of the LIFs for VS1, Host A can establish a connection with any of the LIFs in VS1 as shown in step 2. Host A is not aware of any of the LIFs in VS2 until the management LIF VS2_mgmt_LIF for VS2 registers with the iSNS server.
However, if you define the interface access lists, the host can only use the defined LIFs in the interface access list to access the target.

After iSNS is initially configured, ONTAP automatically updates the iSNS server when the SVM configuration settings change.

A delay of a few minutes can occur between the time you make the configuration changes and when ONTAP sends the update to the iSNS server. Force an immediate update of the iSNS information on the iSNS server:

```
vserver iscsi isns update
```

### Commands for managing iSNS

ONTAP provides commands to manage your iSNS service.

<table>
<thead>
<tr>
<th>If you want to…</th>
<th>Use this command…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure an iSNS service</td>
<td><code>vserver iscsi isns create</code></td>
</tr>
<tr>
<td>Start an iSNS service</td>
<td><code>vserver iscsi isns start</code></td>
</tr>
<tr>
<td>Modify an iSNS service</td>
<td><code>vserver iscsi isns modify</code></td>
</tr>
<tr>
<td>Display iSNS service configuration</td>
<td><code>vserver iscsi isns show</code></td>
</tr>
<tr>
<td>Force an update of registered iSNS information</td>
<td><code>vserver iscsi isns update</code></td>
</tr>
<tr>
<td>If you want to...</td>
<td>Use this command...</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>Stop an iSNS service</td>
<td>vserver iscsi isns stop</td>
</tr>
<tr>
<td>Remove an iSNS service</td>
<td>vserver iscsi isns delete</td>
</tr>
<tr>
<td>View the man page for a command</td>
<td>man command name</td>
</tr>
</tbody>
</table>

See the man page for each command for more information.