NetApp

Manage iSCSI protocol

ONTAP 9

NetApp
June 28, 2022

Table of Contents

Manage iSCSI protocol

Configure your network for best performance

Ethernet networks vary greatly in performance. You can maximize the performance of the network used for iSCSI by selecting specific configuration values.

Steps

1. Connect the host and storage ports to the same network.

   It is best to connect to the same switches. Routing should never be used.

2. Select the highest speed ports available, and dedicate them to iSCSI.

   10 GbE ports are best. 1 GbE ports are the minimum.

3. Disable Ethernet flow control for all ports.

   You should see the *ONTAP 9 Network Management Guide* for using the CLI to configure Ethernet port flow control.

   Network management

4. Enable jumbo frames (typically MTU of 9000).

   All devices in the data path, including initiators, targets, and switches, must support jumbo frames. Otherwise, enabling jumbo frames actually reduces network performance substantially.

Define a security policy method for an initiator

You can define a list of initiators and their authentication methods. You can also modify the default authentication method that applies to initiators that do not have a user-defined authentication method.

About this task

You can generate unique passwords using security policy algorithms in the product or you can manually specify the passwords that you want to use.

ⓘ Not all initiators support hexadecimal CHAP secret passwords.

Steps

1. Use the `vserver iscsi security create` command to create a security policy method for an initiator.

   ```
   vserver iscsi security create -vserver vs2 -initiator iqn.1991-
   05.com.microsoft:host1 -auth-type CHAP -user-name bob1 -outbound-user-name
   bob2
   ```

2. Follow the screen commands to add the passwords.

Creates a security policy method for initiator iqn.1991-05.com.microsoft:host1 with inbound and outbound CHAP user names and passwords.

Related information

- How iSCSI authentication works
- Guidelines for using CHAP authentication
- What CHAP authentication is

Delete an iSCSI service for an SVM

You can delete an iSCSI service for a storage virtual machine (SVM) if it is no longer required.

What you'll need

The administration status of the iSCSI service must be in the "down" state before you can delete an iSCSI service. You can move the administration status to down with the `vserver iscsi modify` command.

Steps

1. Use the `vserver iscsi modify` command to stop the I/O to the LUN.

   `vserver iscsi modify -vserver vs1 -status-admin down`

2. Use the `vserver iscsi delete` command to remove the iscsi service from the SVM.

   `vserver iscsi delete -vserver vs_1`

3. Use the `vserver iscsi show command` to verify that you deleted the iSCSI service from the SVM.

   `vserver iscsi show -vserver vs1`

Get more details in iSCSI session error recoveries

Increasing the iSCSI session error recovery level enables you to receive more detailed information about iSCSI error recoveries. Using a higher error recovery level might cause a minor reduction in iSCSI session performance.

About this task

By default, ONTAP is configured to use error recovery level 0 for iSCSI sessions. If you are using an initiator that has been qualified for error recovery level 1 or 2, you can choose to increase the error recovery level. The modified session error recovery level affects only the newly created sessions and does not affect existing sessions.

Beginning with ONTAP 9.4, the `max-error-recovery-level` option is not supported in the `iscsi show` and `iscsi modify` commands.

Steps

1. Enter advanced mode:

```
set -privilege advanced
```

2. Verify the current setting by using the `iscsi show` command.

```
iscsi show -vserver vs3 -fields max-error-recovery-level
```

```
vserver max-error-recovery-level
------- ------------------------
vs3       0
```

3. Change the error recovery level by using the `iscsi modify` command.

```
iscsi modify -vserver vs3 -max-error-recovery-level 2
```

Register the SVM with an iSNS server

You can use the `vserver iscsi isns` command to configure the storage virtual machine (SVM) to register with an iSNS server.

About this task

The `vserver iscsi isns create` command configures the SVM to register with the iSNS server. The SVM does not provide commands that enable you to configure or manage the iSNS server. To manage the iSNS server, you can use the server administration tools or the interface provided by the vendor for the iSNS server.

Steps

1. On your iSNS server, ensure that your iSNS service is up and available for service.

2. Create the SVM management LIF on a data port:

```
network interface create -vserver SVM_name -lif lif_name -role data -data
-protocol none -home-node home_node_name -home-port home_port -address
IP_address -netmask network_mask
```

3. Create an iSCSI service on your SVM if one does not already exist:

```
vserver iscsi create -vserver SVM_name
```

4. Verify that the iSCSI service was created successfully:

```
iscsi show -vserver SVM_name
```

5. Verify that a default route exists for the SVM:

```
network route show -vserver SVM_name
```

6. If a default route does not exist for the SVM, create a default route:

```
network route create -vserver SVM_name -destination destination -gateway
gateway
```

7. Configure the SVM to register with the iSNS service:

```
vserver iscsi isns create -vserver SVM_name -address IP_address
```

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

For example, you cannot connect anSVM management LIF with an IPv4 address to an iSNS server with an IPv6 address.

8. Verify that the iSNS service is running:

```
vserver iscsi isns show -vserver SVM_name
```

9. If the iSNS service is not running, start it:

```
vserver iscsi isns start -vserver SVM_name
```

Resolve iSCSI error messages on the storage system

There are a number of common iSCSI-related error messages that you can view with the `event log show` command. You need to know what these messages mean and what you can do to resolve the issues they identify.

The following table contains the most common error messages, and instructions for resolving them:

Message	Explanation	What to do
`ISCSI: network interface identifier disabled for use; incoming connection discarded`	The iSCSI service is not enabled on the interface.	You can use the `iscsi interface enable` command to enable the iSCSI service on the interface. For example: `iscsi interface enable -vserver vs1 -lif lif1`
`ISCSI: Authentication failed for initiator nodename`	CHAP is not configured correctly for the specified initiator.	You should check the CHAP settings; you cannot use the same user name and password for inbound and outbound settings on the storage system: • Inbound credentials on the storage system must match outbound credentials on the initiator. • Outbound credentials on the storage system must match inbound credentials on the initiator.

Troubleshoot iSCSI LUNs not visible on the host

The iSCSI LUNs appear as local disks to the host. If the storage system LUNs are not available as disks on the host, you should verify the configuration settings.

Configuration setting	What to do
Cabling	Verify that the cables between the host and storage system are properly connected.
Network connectivity	Verify that there is TCP/IP connectivity between the host and storage system. • From the storage system command line, ping the host interfaces that are being used for iSCSI: `ping -node node_name -destination host_ip_address_for_iSCSI` • From the host command line, ping the storage system interfaces that are being used for iSCSI: `ping -node node_name -destination host_ip_address_for_iSCSI`
System requirements	Verify that the components of your configuration are qualified. Also, verify that you have the correct host operating system (OS) service pack level, initiator version, ONTAP version, and other system requirements. The Interoperability Matrix contains the most up-to-date system requirements.
Jumbo frames	If you are using jumbo frames in your configuration, verify that jumbo frames are enabled on all devices in the network path: the host Ethernet NIC, the storage system, and any switches.
iSCSI service status	Verify that the iSCSI service is licensed and started on the storage system.
Initiator login	Verify that the initiator is logged in to the storage system. If the `iscsi initiator show` command output shows no initiators are logged in, check the initiator configuration on the host. Also verify that the storage system is configured as a target of the initiator.
iSCSI node names (IQNs)	Verify that you are using the correct initiator node names in the igroup configuration. On the host, you can use the initiator tools and commands to display the initiator node name. The initiator node names configured in the igroup and on the host must match.

Configuration setting	What to do
LUN mappings	Verify that the LUNs are mapped to an igroup. On the storage system console, you can use one of the following commands: • `lun mapping show` displays all LUNs and the igroups to which they are mapped. • `lun mapping show -igroup` displays the LUNs mapped to a specific igroup.
iSCSI LIFs enable	Verify that the iSCSI logical interfaces are enabled.

Related information

NetApp Interoperability Matrix Tool

iSCSI LIF failover for ASA platforms

The iSCSI logical interface (LIF) failover feature is available from ONTAP 9.11.1 on All SAN Array (ASA) platforms and allows iSCSI LIFs to migrate from the node which is going down to its HA partner before the home-node goes down. The iSCSI LIF failover feature can only be enabled after the entire ONTAP cluster is on ONTAP 9.11.1 or later.

About this task

The following list describes how this feature works:

• For LIFs using the `data-iscsi` service policy, the failover-policy is restricted to `sfo-partner-only`, `local-only`, and `disabled`

• iSCSI LIFs can failover only to the HA partner when their failover policy is set to `sfo-partner-only`

• Giveback happens when the giveback policy is set to `auto-revert true` and the node comes back in quorum

• When there is a planned or unplanned node takeover, the iSCSI LIF on the node which is taken-over fails over to the HA partner; the port on which the LIF fails over is determined by the VIF Manager

• Once the failover is complete, the iSCSI LIF operates normally

• When a giveback is initiated, the iSCSI LIF reverts back to its home node and port

System Manager procedure

Beginning with ONTAP 9.11.1, you can use System Manager to migrate an iSCSI LIF from an ASA platform which is going down to its HA partner before the home-node goes down. The ability to migrate and revert are enabled by default on ASA platforms.

Failover

Steps

1. In System Manager, click **Network > Overview > Network Interfaces**

2. Select the LIF you want to migrate, then click ⋮, and then click **Migrate**.

3. In the **Migrate Interface** dialog box, select the destination node and port of the HA partner.

4. Click **Migrate**.

Giveback

Steps

1. In System Manager, click **Network > Overview > Network Interfaces**.

2. Select the LIF you want to revert, then click ⋮ and then click **Revert Network Interface**.

3. In the **Revert Network Interface** dialog box, click **Revert**.

CLI procedure

Beginning with ONTAP 9.11.1, use the following commands on an ASA platform, to create and manage iSCSI LIFs. The ability to failover and auto-revert are enabled by default._

If you want to…	Use this command…
Create an iSCSI LIF	`network interface create -vserver` *SVM_name* `-lif` *iscsi_lif* `-service-policy default-data-blocks -data-protocol iscsi -home-node` *node_name* `-home-port` *port_name*
Verify that the LIF was created successfully	`network interface show -vserver` *SVM_name* `-fields failover-policy,failover-group,auto-revert,is-home`
Verify if you can override the auto-revert default on iSCSI LIFs	`network interface modify -vserver` *SVM_name* `-lif iscsi_lif -auto-revert false` You will receive an error: `Error: command failed: auto-revert cannot be disabled on SAN LIFs.`
Perform a storage failover on an iSCSI LIF	`storage failover takeover -ofnode` *node_name* `-option normal` You will receive a warning: `A takeover will be initiated. Once the partner node reboots, a giveback will be automatically initiated. Do you want to continue? {y/n}:` A `y` response will display a takeover message from its HA partner.