



Manage iSCSI protocol

ONTAP 9

NetApp
January 29, 2024

Table of Contents

- Manage iSCSI protocol 1
 - Configure your network for best performance 1
 - Configure an SVM for iSCSI 1
 - Define a security policy method for an initiator 3
 - Delete an iSCSI service for an SVM 3
 - Get more details in iSCSI session error recoveries 4
 - Register the SVM with an iSNS server 4
 - Resolve iSCSI error messages on the storage system 5
 - Enable or disable automatic iSCSI LIF failover 6

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 [Network management](#) for using the CLI to configure Ethernet port flow control.

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.

Configure an SVM for iSCSI

To configure a storage virtual machine (SVM) for iSCSI, you must create LIFs for the SVM and assign the iSCSI protocol to those LIFs.

About this task

You need a minimum of one iSCSI LIF per node for each SVM serving data with the iSCSI protocol. For redundancy, you should create at least two LIFs per node.

Example 1. Steps

System Manager

Configure an storage VM for iSCSI with ONTAP System Manager (9.7 and later).

To configure iSCSI on a new storage VM	To configure iSCSI on an existing storage VM
<ol style="list-style-type: none">1. In System Manager, click Storage > Storage VMs and then click Add.2. Enter a name for the storage VM.3. Select iSCSI for the Access Protocol.4. Click Enable iSCSI and enter the IP address and subnet mask for the network interface. + Each node should have at least two network interfaces.5. Click Save.	<ol style="list-style-type: none">1. In System Manager, click Storage > Storage VMs.2. Click on the storage VM you want to configure.3. Click on the Settings tab, and then click  next to the iSCSI protocol.4. Click Enable iSCSI and enter the IP address and subnet mask for the network interface. + Each node should have at least two network interfaces.5. Click Save.

CLI

Configure an storage VM for iSCSI with the ONTAP CLI.

1. Enable the SVMs to listen for iSCSI traffic:

```
vserver iscsi create -vserver vserver_name -target-alias vserver_name
```

2. Create a LIF for the SVMs on each node to use for iSCSI:

- For ONTAP 9.6 and later:

```
network interface create -vserver vserver_name -lif lif_name -data  
-protocol iscsi -service-policy default-data-iscsi -home-node node_name  
-home-port port_name -address ip_address -netmask netmask
```

- For ONTAP 9.5 and earlier:

```
network interface create -vserver vserver_name -lif lif_name -role data  
-data-protocol iscsi -home-node node_name -home-port port_name -address  
ip_address -netmask netmask
```

3. Verify that you set up your LIFs correctly:

```
network interface show -vserver vserver_name
```

4. Verify that iSCSI is up and running and the target IQN for that SVM:

```
vserver iscsi show -vserver vserver_name
```

5. From your host, create iSCSI sessions to your LIFs.

Related information

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](#)
- [CHAP authentication](#)

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 an SVM 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.	<p>You can use the <code>iscsi interface enable</code> command to enable the iSCSI service on the interface. For example:</p> <pre>iscsi interface enable -vserver vs1 -lif lif1</pre>
ISCSI: Authentication failed for initiator nodename	CHAP is not configured correctly for the specified initiator.	<p>You should check the CHAP settings; you cannot use the same user name and password for inbound and outbound settings on the storage system:</p> <ul style="list-style-type: none"> • 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.

Enable or disable automatic iSCSI LIF failover

After you upgrade to ONTAP 9.11.1 or later, you should manually enable automatic LIF failover on all iSCSI LIFs created in ONTAP 9.10.1 or earlier.

Beginning with ONTAP 9.11.1, you can enable automatic LIF failover for iSCSI LIFs on All-flash SAN Array platforms. If a storage failover occurs, the iSCSI LIF is automatically migrated from its home node or port to its HA partner node or port and then back once the failover is complete. Or, if the port for iSCSI LIF becomes unhealthy, the LIF is automatically migrated to a healthy port in its current home node and then back to its original port once the port is healthy again. This enables SAN workloads running on iSCSI to resume I/O service faster after a failover is experienced.

In ONTAP 9.11.1 and later, by default, newly created iSCSI LIFs are enabled for automatic LIF failover if one of the following conditions is true:

- There are no iSCSI LIFs on the SVM
- All iSCSI LIFs on the SVM are enabled for automatic LIF failover

Enable automatic iSCSI LIF failover

By default, iSCSI LIFs created in ONTAP 9.10.1 and earlier are not enabled for automatic LIF failover. If there are iSCSI LIFs on the SVM that are not enabled for automatic LIF failover, your newly created LIFs will not be enabled for automatic LIF failover either. If automatic LIF failover is not enabled and there is a failover event your iSCSI LIFs will not migrate.

Learn more about [LIF failover and giveback](#).

Step

1. Enable automatic failover for an iSCSI LIF:

```
network interface modify -vserver SVM_name -lif iscsi_lif -failover-policy sfo-partner-only -auto-revert true
```

To update all iSCSI LIFs on the SVM, use `-lif*` instead of `lif`.

Disable automatic iSCSI LIF failover

If you previously enabled automatic iSCSI LIF failover on iSCSI LIFs created in ONTAP 9.10.1 or earlier, you have the option to disable it.

Step

1. Disable automatic failover for an iSCSI LIF:

```
network interface modify -vserver SVM_name -lif iscsi_lif -failover-policy disabled -auto-revert false
```

To update all iSCSI LIFs on the SVM, use `-lif*` instead of `lif`.

Related Information

- [Create a LIF](#)
- Manually [migrate a LIF](#)
- Manually [revert a LIF to its home port](#)
- [Configure failover settings on a LIF](#)

Copyright information

Copyright © 2024 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.