



iSCSI protocol

System Manager Classic

NetApp
January 13, 2022

Table of Contents

- iSCSI protocol 1
 - Create iSCSI aliases 1
 - Enabling or disabling the iSCSI service on storage system interfaces 1
 - Add the security method for iSCSI initiators 2
 - Editing default security settings 2
 - Editing initiator security 3
 - Changing the default iSCSI initiator authentication method 3
 - Setting the default security for iSCSI initiators 4
 - Starting or stopping the iSCSI service 4
 - Viewing initiator security information 4
- iSCSI window 5

iSCSI protocol

You can use System Manager to configure the iSCSI protocol that enables you to transfer block data to hosts using SCSI protocol over TCP/IP.

Related information

[SAN administration](#)

Create iSCSI aliases

An iSCSI alias is a user-friendly identifier that you assign to an iSCSI target device (in this case, the storage system) to make it easier to identify the target device in user interfaces. You can use System Manager to create an iSCSI alias.

About this task

An iSCSI alias is a string of 1 to 128 printable characters. An iSCSI alias must not include spaces.

Steps

1. Click **Storage > SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Protocols** pane, click **iSCSI**.
4. In the **Service** tab of the **iSCSI** window, click **Edit**.
5. In the **Edit iSCSI Service Configuration** dialog box, enter an iSCSI alias in the **Target Alias** field, and then click **OK**.

Related information

[iSCSI window](#)

Enabling or disabling the iSCSI service on storage system interfaces

You can use System Manager to control which network interfaces are used for iSCSI communication by enabling or disabling the interfaces. When the iSCSI service is enabled, iSCSI connections and requests are accepted over those network interfaces that are enabled for iSCSI, but not over disabled interfaces.

Before you begin

You must have terminated any outstanding iSCSI connections and sessions that are currently using the interface. By default, the iSCSI service is enabled on all of the Ethernet interfaces after you enable the iSCSI license.

Steps

1. Click **Storage > SVMs**.
2. Select the SVM, and then click **SVM Settings**.

3. In the **Protocols** pane, click **iSCSI**.
4. In the **iSCSI Interfaces** area, select the interface on which you want to enable or disable the iSCSI service.
5. Click **Enable** or **Disable**, as required.

Related information

[iSCSI window](#)

[Configuring iSCSI protocol on SVMs](#)

Add the security method for iSCSI initiators

You can use System Manager to add an initiator and to specify the security method that is used to authenticate the initiator.

Steps

1. Click **Storage > SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Protocols** pane, click **iSCSI**.
4. In the **iSCSI** window, click the **Initiator Security** tab.
5. Click **Add** in the **Initiator Security** area.
6. Specify the initiator name and the security method for authenticating the initiator.

For CHAP authentication, you must provide the user name and password, and then confirm your password for inbound settings. For outbound settings, this login information is optional.

7. Click **OK**.

Related information

[iSCSI window](#)

Editing default security settings

You can use the Edit Default Security dialog box in System Manager to edit the default security settings for the iSCSI initiators that are connected to the storage system.

Steps

1. Click **Storage > SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Protocols** pane, click **iSCSI**.
4. In the **Default Security** area of the **Initiator Security** tab, click **Edit**.
5. In the **Edit Default Security** dialog box, change the security type.

For CHAP authentication, you must provide the user name and password, and then confirm your password for inbound settings. For outbound settings, this login information is optional.

6. Click **OK**.

Related information

[iSCSI window](#)

Editing initiator security

The security style that is configured for an initiator specifies how authentication is done for that initiator during the iSCSI connection login phase. You can use System Manager to change the security for selected iSCSI initiators by changing the authentication method.

Steps

1. Click **Storage > SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Protocols** pane, click **iSCSI**.
4. In the **Initiator Security** tab, select one or more initiators from the initiator list, and then click **Edit** in the **Initiator Security** area.
5. Change the security type.

For CHAP authentication, you must provide the user name and password, and then confirm your password for inbound settings. For outbound settings, this login information is optional.

6. Click **OK**.
7. Verify the changes that you made in the **Initiator Security** tab.

Related information

[iSCSI window](#)

Changing the default iSCSI initiator authentication method

You can use System Manager to change the default iSCSI authentication method, which is the authentication method that is used for any initiator that is not configured with a specific authentication method.

Steps

1. Click **Storage > SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Protocols** pane, click **iSCSI**.
4. In the **Initiator Security** tab, click **Edit** in the **Default Security** area.
5. Change the security type.

For CHAP authentication, you must provide the user name and password, and then confirm your password for inbound settings. For outbound settings, this login information is optional.

6. Click **OK**.

Related information

[iSCSI window](#)

Setting the default security for iSCSI initiators

You can use System Manager to remove the authentication settings for an initiator and to use the default security method to authenticate the initiator.

Steps

1. Click **Storage > SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Protocols** pane, click **iSCSI**.
4. In the **Initiator Security** tab, select the initiator for which you want to change the security setting.
5. Click **Set Default** in the **Initiator Security** area, and then click **Set Default** in the confirmation dialog box.

Related information

[iSCSI window](#)

Starting or stopping the iSCSI service

You can use System Manager to start or stop the iSCSI service on your storage system.

Steps

1. Click **Storage > SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Protocols** pane, click **iSCSI**.
4. Click **Start** or **Stop**, as required.

Related information

[iSCSI window](#)

Viewing initiator security information

You can use System Manager to view the default authentication information and all the initiator-specific authentication information.

Steps

1. Click **Storage > SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Protocols** pane, click **iSCSI**.
4. In the **Initiator Security** tab of the **iSCSI** window, review the details.

iSCSI window

You can use the iSCSI window to start or stop the iSCSI service, change a storage system iSCSI node name, and create or change the iSCSI alias of a storage system. You can also add or change the initiator security setting for an iSCSI initiator that is connected to your storage system.

Tabs

- **Service**

You can use the **Service** tab to start or stop the iSCSI service, change a storage system iSCSI node name, and create or change the iSCSI alias of a storage system.

- **Initiator Security**

You can use the **Initiator Security** tab to add or change the initiator security setting for an iSCSI initiator that is connected to your storage system.

Command buttons

- **Edit**

Opens Edit iSCSI Service Configurations dialog box, which enables you to change iSCSI node name and iSCSI alias of the storage system.

- **Start**

Starts the iSCSI service.

- **Stop**

Stops the iSCSI service.

- **Refresh**

Updates the information in the window.

Details area

The details area displays information about the status of the iSCSI service, iSCSI target node name, and iSCSI target alias. You can use this area to enable or disable the iSCSI service on a network interface.

Related information

[Creating iSCSI aliases](#)

[Enabling or disabling the iSCSI service on storage system interfaces](#)

[Adding the security method for iSCSI initiators](#)

[Editing default security settings](#)

Editing initiator security

Changing the default iSCSI initiator authentication method

Setting the default security for iSCSI initiators

Starting or stopping the iSCSI service

Copyright Information

Copyright © 2022 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.