Export policies

System Manager Classic

NetApp
December 09, 2021

This PDF was generated from https://docs.netapp.com/us-en/ontap-sm-classic/online-help-96-97/task_creating_export_policy.html on December 09, 2021. Always check docs.netapp.com for the latest.

Table of Contents

Export policies . . . 1
- Create an export policy . . . 1
- Renaming export policies . . . 1
- Deleting export policies . . . 1
- Add rules to an export policy . . . 2
- Modifying export policy rules . . . 3
- Deleting export policy rules . . . 3
- How export policies control client access to volumes or qtrees . . . 3
- Export Policies window . . . 4

Export policies

You can use System Manager to create, edit, and manage export policies.

Create an export policy

You can use System Manager to create an export policy so that clients can access specific volumes.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Policies** pane, click **Export Policies**.
4. Click **Create**.
5. In the **Create Export Policy** dialog box, specify a name for the export policy.
6. If you want to create an export policy by copying the rules from an existing export policy, select the **Copy Rules from** check box, and then select the storage virtual machine (SVM) and the export policy.

   You should not select the destination SVM for disaster recovery from the drop-down menu to create an export policy.

7. In the **Export Rules**area, click **Add** to add rules to the export policy.
8. Click **Create**.
9. Verify that the export policy that you created is displayed in the **Export Policies** window.

Renaming export policies

You can use System Managerto rename an existing export policy.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Policies** pane, click **Export Policies**.
4. Select the export policy that you want to rename, and then click **Rename Policy**.
5. In the **Rename Policy** dialog box, specify a new policy name, and then click **Modify**.
6. Verify the changes that you made in the **Export Policies** window.

Deleting export policies

You can use System Manager to delete export policies that are no longer required.

Steps

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

3. In the **Policies** pane, click **Export Policies**.
4. Select the export policy that you want to delete, and then click **Delete Policy**.
5. Select the confirmation check box, and then click **Delete**.

Add rules to an export policy

You can use System Manager to add rules to an export policy, which enables you to define client access to data.

Before you begin

You must have created the export policy to which you want to add the export rules.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Policies** pane, click **Export Policies**.
4. Select the export policy to which you want to add rules, and from the **Export Rules** tab, click **Add**.
5. In the **Create Export Rule** dialog box, perform the following steps:

   a. Specify the client that requires access to the data.

      You can specify multiple clients as comma-separated values.

      You can specify the client in any of the following formats:

      - As a host name; for instance, host1
      - As an IPv4 address; for instance, 10.1.12.24
      - As an IPv4 address with a network mask; for instance, 10.1.16.0/255.255.255.0
      - As an IPv6 address; for instance, FE80::0202:B3FF:FE1E:8329
      - As an IPv6 address with a network mask; for instance, 2001:db8::/32
      - As a netgroup, with the netgroup name preceded by an at symbol (@); for instance, @netgroup
      - As a domain name preceded by a period (.); for instance, .example.com

      You must not enter an IP address range, such as 10.1.12.10 through 10.1.12.70. Entries in this format are interpreted as a text string and are treated as a host name.

   + You can enter the IPv4 address `0.0.0.0/0` to provide access to all of the hosts.

   a. If you want to modify the rule index number, select the appropriate rule index number.
   b. Select one or more access protocols.

      If you do not select any access protocol, the default value “Any” is assigned to the export rule.

   c. Select one or more security types and access rules.
6. Click **OK**.
7. Verify that the export rule that you added is displayed in the **Export Rules** tab for the selected export

policy.

Modifying export policy rules

You can use System Manager to modify the specified client, access protocols, and access permissions of an export policy rule.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Policies** pane, click **Export Policies**.
4. In the **Export Policies** window, select the export policy for which you want to edit the export rule, and in the **Export Rules** tab, select the rule that you want to edit, and then click **Edit**.
5. Modify the following parameters as required:
   - Client specification
   - Access protocols
   - Access details
6. Click **OK**.
7. Verify that the updated changes for the export rule are displayed in the **Export Rules** tab.

Related information

Setting up CIFS

Deleting export policy rules

You can use System Manager to delete export policy rules that are no longer required.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Policies** pane, click **Export Policies**.
4. Select the export policy for which you want to delete the export rule.
5. In the **Export Rules** tab, select the export rule that you want to delete, and then click **Delete**.
6. In the confirmation box, click **Delete**.

How export policies control client access to volumes or qtrees

Export policies contain one or more *export rules* that process each client access request. The result of the process determines whether the client is denied or granted access and what level of access. An export policy with export rules must exist on the storage virtual machine (SVM) for clients to access data.

You associate exactly one export policy with each volume or qtree to configure client access to the volume or qtree. The SVM can contain multiple export policies. This enables you to do the following for SVMs with multiple volumes or qtrees:

- Assign different export policies to each volume or qtree of the SVM for individual client access control to each volume or qtree in the SVM.
- Assign the same export policy to multiple volumes or qtrees of the SVM for identical client access control without having to create a new export policy for each volume or qtree.

If a client makes an access request that is not permitted by the applicable export policy, the request fails with a permission-denied message. If a client does not match any rule in the export policy, then access is denied. If an export policy is empty, then all accesses are implicitly denied.

You can modify an export policy dynamically on a system running ONTAP.

Export Policies window

You can use the Export Policies window to create, view, and manage information about export policies and its related export rules.

Export Policies

The Export Policies window enables you to view and manage the export policies created for the storage virtual machine (SVM).

- **Command buttons**
  - Create

    Opens the Create Export Policy dialog box, which enables you to create an export policy and add export rules. You can also copy export rules from an existing SVM.

  - Rename

    Opens the Rename Policy dialog box, which enables you to rename the selected export policy.

  - Delete

    Opens the Delete Export Policy dialog box, which enables you to delete the selected export policy.

  - Refresh

    Updates the information in the window.

Export Rules tab

The Export Rules tab enables you to view information about the export rules created for a particular export policy. You can also add, edit, and delete rules.

- **Command buttons**
  - Add

    Opens the Create Export Rule dialog box, which enables you to add an export rule to the selected

export policy.

- Edit

  Opens the Modify Export Rule dialog box, which enables you to modify the attributes of the selected export rule.

- Delete

  Opens the Delete Export Rule dialog box, which enables you to delete the selected export rule.

- Move Up

  Moves up the rule index of the selected export rule.

- Move Down

  Moves down the rule index of the selected export rule.

- Refresh

  Updates the information in the window.

- **Export rules list**
  - Rule Index

    Specifies the priority based on which the export rules are processed. You can use the Move Up and Move Down buttons to choose the priority.

  - Client

    Specifies the client to which the rule applies.

  - Access Protocols

    Displays the access protocol that is specified for the export rule.

    If you have not specified any access protocol, the default value “Any” is considered.

  - Read-Only Rule

    Specifies one or more security types for read-only access.

  - Read/Write Rule

    Specifies one or more security types for read/write access.

  - Superuser Access

    Specifies the security type or types for superuser access.

Assigned Objects tab

The Assigned Objects tab enables you to view the volumes and qtrees that are assigned to the selected export policy. You can also view whether the volume is encrypted or not.

Copyright Information

Copyright © 2021 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.