



Add an NFS volume to an NFS-enabled SVM

System Manager Classic

NetApp
December 09, 2021

This PDF was generated from https://docs.netapp.com/us-en/ontap-sm-classic/nfs-config/task_creating_configuring_volume.html on December 09, 2021. Always check docs.netapp.com for the latest.

Table of Contents

- Add an NFS volume to an NFS-enabled SVM 1
 - Create and configure a volume 1
 - Create an export policy for the volume 2
 - Verify NFS access from a UNIX administration host 4
 - Configure and verify NFS client access (Add an NFS volume to an NFS-enabled SVM) 5

Add an NFS volume to an NFS-enabled SVM

Adding an NFS volume to an NFS-enabled SVM involves creating and configuring a volume, creating an export policy, and verifying access from a UNIX administration host. You can then configure NFS client access.

Before you begin

NFS must be completely set up on the SVM.

Create and configure a volume

You must create a FlexVol volume to contain your data. You can optionally change the volume's default security style, which is inherited from the security style of the root volume. You can also optionally change the volume's default location in the namespace, which is at the root volume of the storage virtual machine (SVM).

Steps

1. Navigate to the **Volumes** window.
2. Click **Create > Create FlexVol**.

The Create Volume dialog box is displayed.

3. If you want to change the default name, which ends in a date and time stamp, specify a new name, such as `vol1`.
4. Select an aggregate for the volume.
5. Specify the size of the volume.
6. Click **Create**.

Any new volume created in System Manager is mounted by default at the root volume using the volume name as the junction name. NFS clients use the junction path and the junction name when mounting the volume.

7. If you do not want the volume to be located at the root of the SVM, modify the place of the new volume in the existing namespace:
 - a. Navigate to the **Namespace** window.
 - b. Select the **SVM** from the drop-down menu.
 - c. Click **Mount**.
 - d. In the **Mount Volume** dialog box, specify the volume, the name of its junction path, and the junction path on which you want the volume mounted.
 - e. Verify the new junction path in the **Namespace** window.

If you want to organize certain volumes under a main volume named "data", you can move the new volume "vol1" from the root volume to the "data" volume.

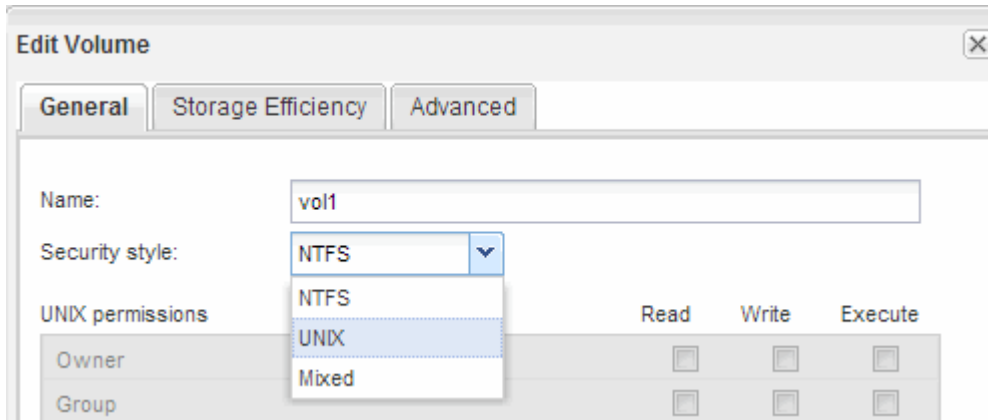
+ image::.../media/namespace_1_before_nfs.gif[This graphic is described by the surrounding text.]

8. Review the volume's security style and change it, if necessary:

- a. In the **Volume** window, select the volume you just created, and click **Edit**.

The Edit Volume dialog box is displayed, showing the volume's current security style, which is inherited from the security style of the SVM root volume.

- b. Make sure the security style is UNIX.



Create an export policy for the volume

Before any NFS clients can access a volume, you must create an export policy for the volume, add a rule that permits access by an administration host, and apply the new export policy to the volume.

Steps

1. Navigate to the **SVMs** window.
2. Click the **SVM Settings** tab.
3. Create a new export policy:
 - a. In the **Policies** pane, click **Export Policies** and then click **Create**.
 - b. In the **Create Export Policy** window, specify a policy name.
 - c. Under **Export Rules**, click **Add** to add a rule to the new policy.

Create Export Policy

Policy Name:

☐ Copy Rules from

Storage Virtual Machine:

Export Policy:

Export Rules:

Rule Index	Client	Access Protocols	Read-Only Rule
------------	--------	------------------	----------------

4. In the **Create Export Rule** dialog box, create a rule that allows an administrator full access to the export through all protocols:
 - a. Specify the IP address or client name, such as `admin_host`, from which the exported volume will be administered.
 - b. Select **NFSv3**.
 - c. Ensure that all **Read/Write** access details are selected, as well as **Allow Superuser Access**.

Create Export Rule

Client Specification:

Access Protocols:

☒ CIFS

☐ NFS ☒ NFSv3 ☐ NFSv4

☐ Flexcache

If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details:

☐ Read-Only ☒ Read/Write

UNIX	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5i	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NTLM	<input type="checkbox"/>	<input checked="" type="checkbox"/>

☒ Allow Superuser Access

Superuser access is set to all

- d. Click **OK** and then click **Create**.

The new export policy is created, along with its new rule.

5. Apply the new export policy to the new volume so that the administrator host can access the volume:

- a. Navigate to the **Namespace** window.
- b. Select the volume and click **Change Export Policy**.
- c. Select the new policy and click **Change**.

Related information

[Verifying NFS access from a UNIX administration host](#)

Verify NFS access from a UNIX administration host

After you configure NFS access to storage virtual machine (SVM), you should verify the configuration by logging in to an NFS administration host and reading data from and writing data to the SVM.

Before you begin

- The client system must have an IP address that is allowed by the export rule you specified earlier.
- You must have the login information for the root user.

Steps

1. Log in as the root user to the client system.
2. Enter `cd /mnt/` to change the directory to the mount folder.
3. Create and mount a new folder using the IP address of the SVM:
 - a. Enter `mkdir /mnt/folder` to create a new folder.
 - b. Enter `mount -t nfs -o nfsvers=3,hard IPAddress:/volume_name /mnt/folder` to mount the volume at this new directory.
 - c. Enter `cd folder` to change the directory to the new folder.

The following commands create a folder named `test1`, mount the `vol1` volume at the `192.0.2.130` IP address on the `test1` mount folder, and change to the new `test1` directory:

```
host# mkdir /mnt/test1
host# mount -t nfs -o nfsvers=3,hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

4. Create a new file, verify that it exists, and write text to it:
 - a. Enter `touch filename` to create a test file.
 - b. Enter `ls -l filename` to verify that the file exists.
 - c. Enter `cat >filename`, type some text, and then press `Ctrl+D` to write text to the test file.
 - d. Enter `cat filename` to display the content of the test file.
 - e. Enter `rm filename` to remove the test file.
 - f. Enter `cd ..` to return to the parent directory.

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

Results

You have confirmed that you have enabled NFS access to the SVM.

Configure and verify NFS client access (Add an NFS volume to an NFS-enabled SVM)

When you are ready, you can give select clients access to the share by setting UNIX file permissions on a UNIX administration host and adding an export rule in System Manager. Then you should test that the affected users or groups can access the volume.

Steps

1. Decide which clients and users or groups will be given access to the share.
2. On a UNIX administration host, use the root user to set UNIX ownership and permissions on the volume.
3. In System Manager, add rules to the export policy to permit NFS clients to access the share.
 - a. Select the storage virtual machine (SVM), and click **SVM Settings**.
 - b. In the **Policies** pane, click **Export Policies**.
 - c. Select the export policy with the same name as the volume.
 - d. In the **Export Rules** tab, click **Add**, and specify a set of clients.
 - e. Select **2** for the **Rule Index** so that this rule executes after the rule that allows access to the administration host.
 - f. Select **NFSv3**.
 - g. Specify the access details that you want, and click **OK**.

You can give full read/write access to clients by typing the subnet `10.1.1.0/24` as the **Client Specification**, and selecting all the access check boxes except **Allow Superuser Access**.

Create Export Rule

Client Specification: 10.1.1.0/24

Rule Index: 2

Access Protocols:

☐ CIFS
☐ NFS
☒ NFSv3
☐ NFSv4
☐ Flexcache

If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details:

☒ Read-Only
☒ Read/Write

UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5i	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
NTLM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Allow Superuser Access	<i>Superuser access is set to all</i>	

- On a UNIX client, log in as one of the users who now has access to the volume, and verify that you can mount the volume and create a file.

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.