



Configure NFS access to an existing SVM

System Manager Classic

NetApp
December 09, 2021

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

Table of Contents

- Configure NFS access to an existing SVM 1
 - Add NFS access to an existing SVM 1
 - Open the export policy of the SVM root volume (Configure NFS access to an existing SVM) 3
 - Configure LDAP (Configure NFS access to an existing SVM) 4
 - Verify NFS access from a UNIX administration host 7
 - Configure and verify NFS client access (Configure NFS access to an existing SVM). 8

Configure NFS access to an existing SVM

Adding access for NFS clients to an existing SVM involves adding NFS configurations to the SVM, opening the export policy of the SVM root volume, optionally configuring LDAP, and verifying NFS access from a UNIX administration host. You can then configure NFS client access.

Add NFS access to an existing SVM

Adding NFS access to an existing SVM involves creating a data LIF, optionally configuring NIS, provisioning a volume, exporting the volume, and configuring the export policy.

Before you begin

- You must know which of the following networking components the SVM will use:
 - The node and the specific port on that node where the data logical interface (LIF) will be created
 - The subnet from which the data LIF's IP address will be provisioned, or optionally the specific IP address you want to assign to the data LIF
- Any external firewalls must be appropriately configured to allow access to network services.
- The NFS protocol must be allowed on the SVM.

<https://docs.netapp.com/us-en/ontap/networking/index.html>

Steps

1. Navigate to the area where you can configure the protocols of the SVM:

- a. Select the SVM that you want to configure.
- b. In the **Details** pane, next to **Protocols**, click **NFS**.

Protocols: NFS FC/FCoE

2. In the **Configure NFS protocol** dialog box, create a data LIF.

- a. Assign an IP address to the LIF automatically from a subnet you specify or manually enter the address.
- b. Click **Browse** and select a node and port that will be associated with the LIF.

Data LIF Configuration

☒ Retain the CIFS data LIF's configuration for NFS clients.

Data Interface details for CIFS

Assign IP Address: Without a subnet

IP Address: 10.224.107.199 [Change](#)

Port: abccorp_1:e0b [Browse...](#)

3. If your site uses NIS for name services or name mapping, specify the domain and IP addresses of the NIS servers and select the database types for which you want to add the NIS name service source.

NIS Configuration {Optional}

Configure NIS domain on the SVM to authorize NFS users.

Domain Names:	<input type="text" value="example.com"/>
IP Addresses:	<input type="text" value="192.0.2.145,192.0.2.146,192.0.2.147"/>

 Database Type: ☒ group ☒ passwd ☒ netgroup

If NIS services are not available, do not attempt to configure it. Improperly configured NIS services can cause datastore access issues.

4. Create and export a volume for NFS access:

- For **Export Name**, type a name that will be both the export name and the beginning of the volume name.
- Specify a size for the volume that will contain the files.

Provision a volume for NFS storage.

Export Name:	<input type="text" value="Eng"/>
Size:	<input type="text" value="10"/> <input type="text" value="GB"/> <input type="button" value="v"/>
Permission:	<input type="text" value="admin_host"/> Change

You do not have to specify the aggregate for the volume because it is automatically located on the aggregate with the most available space.

- In the **Permission** field, click **Change**, and specify an export rule that gives NFSv3 access to a UNIX administration host, including Superuser access.

Create Export Rule


Client Specification:
Enter comma-separated values for multiple client specifications

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:

	<input checked="" type="checkbox"/> Read-Only	<input checked="" type="checkbox"/> Read/Write
UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5i	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5p	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NTLM	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Allow Superuser Access		

Superuser access is set to all

You can create a 10 GB volume named Eng, export it as Eng, and add a rule that gives the “admin_host” client full access to the export, including Superuser access.

5. Click **Submit & Close**, and then click **OK**.

Open the export policy of the SVM root volume (Configure NFS access to an existing SVM)

You must add a rule to the default export policy to allow all clients access through NFSv3. Without such a rule, all NFS clients are denied access to the storage virtual machine (SVM) and its volumes.

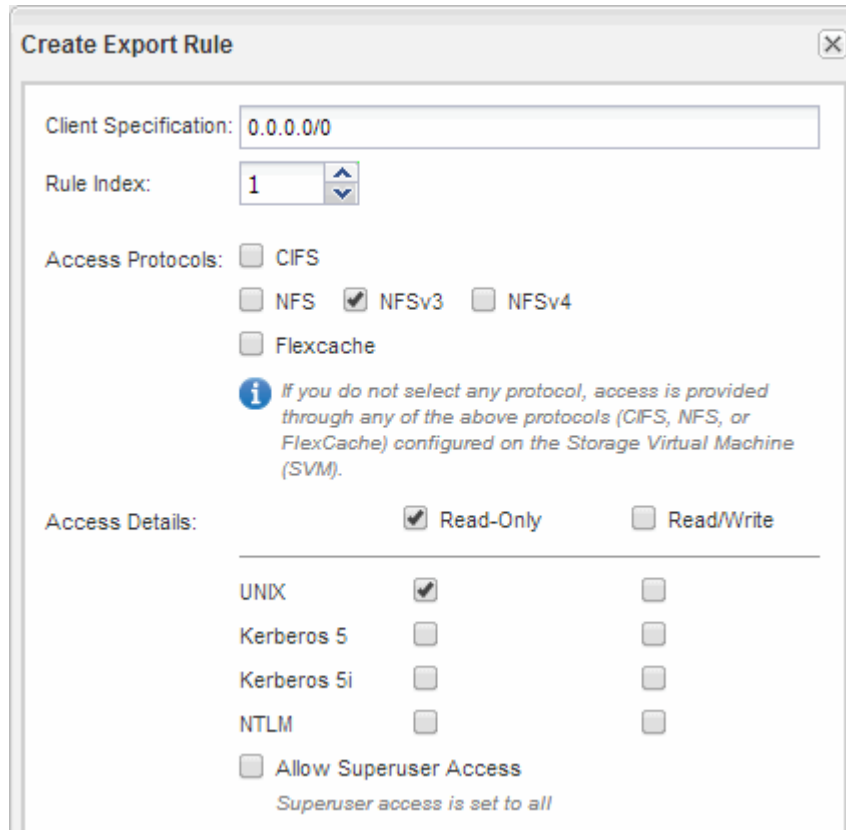
About this task

You should specify all NFS access as the default export policy, and later restrict access to individual volumes by creating custom export policies for individual volumes.

Steps

1. Navigate to the **SVMs** window.
2. Click the **SVM Settings** tab.
3. In the **Policies** pane, click **Export Policies**.
4. Select the export policy named **default**, which is applied to the SVM root volume.
5. In the lower pane, click **Add**.
6. In the **Create Export Rule** dialog box, create a rule that opens access to all clients for NFS clients:
 - a. In the **Client Specification** field, enter `0.0.0.0/0` so that the rule applies to all clients.

- b. Retain the default value as **1** for the rule index.
- c. Select **NFSv3**.
- d. Clear all the check boxes except the **UNIX** check box under **Read-Only**.
- e. Click **OK**.



Create Export Rule

Client Specification: 0.0.0.0/0

Rule Index: 1

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:

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

Results

NFSv3 clients can now access any volumes created on the SVM.

Configure LDAP (Configure NFS access to an existing SVM)

If you want the storage virtual machine (SVM) to get user information from Active Directory-based Lightweight Directory Access Protocol (LDAP), you must create an LDAP client, enable it for the SVM, and give LDAP priority over other sources of user information.

Before you begin

- The LDAP configuration must be using Active Directory (AD).

If you use another type of LDAP, you must use the command-line interface (CLI) and other documentation to configure LDAP.

[NetApp Technical Report 4067: NFS in NetApp ONTAP](#)

[NetApp Technical Report 4616: NFS Kerberos in ONTAP with Microsoft Active Directory](#)

- You must know the AD domain and servers, as well as the following binding information: the authentication level, the Bind user and password, the base DN, and the LDAP port.

Steps

1. Navigate to the **SVMs** window.
2. Select the required SVM
3. Click the **SVM Settings** tab.
4. Set up an LDAP client for the SVM to use:
 - a. In the **Services** pane, click **LDAP Client**.
 - b. In the **LDAP Client Configuration** window, click **Add**.
 - c. In the **General** tab of the **Create LDAP Client** window, type the name of the LDAP client configuration, such as `vs0client1`.
 - d. Add either the AD domain or the AD servers.

The screenshot shows the 'Create LDAP Client' window with the 'General' tab selected. The 'LDAP Client Configuration' field contains 'vs0client1'. Under the 'Servers' section, the 'Active Directory Domain' radio button is selected with the value 'example.com'. Below this, the 'Preferred Active Directory Servers' table lists a single server '192.0.2.145'. To the right of the table are buttons for 'Add', 'Delete', 'Up', and 'Down'. At the bottom, the 'Active Directory Servers' radio button is unselected.

Server
192.0.2.145

- e. Click **Binding**, and specify the authentication level, the Bind user and password, the base DN, and the port.

Edit LDAP Client

General **Binding**

Authentication level:

Bind DN (User):

Bind user password:

Base DN:

Tcp port:

i The Bind Distinguished Name (DN) is the identity which will be used to connect the LDAP server whenever a Storage Virtual Machine requires CIFS user information during data access.

f. Click **Save and Close**.

A new client is created and available for the SVM to use.

5. Enable the new LDAP client for the SVM:

- a. In the navigation pane, click **LDAP Configuration**.
- b. Click **Edit**.
- c. Ensure that the client you just created is selected in **LDAP client name**.
- d. Select **Enable LDAP client**, and click **OK**.

Active LDAP Client

LDAP client name:

☒ Enable LDAP client

Active Directory Domain:

Servers

The SVM uses the new LDAP client.

6. Give LDAP priority over other sources of user information, such as Network Information Service (NIS) and local users and groups:

- a. Navigate to the **SVMs** window.
- b. Select the SVM and click **Edit**.
- c. Click the **Services** tab.
- d. Under **Name Service Switch**, specify **LDAP** as the preferred name service switch source for the database types.
- e. Click **Save and Close**.

Edit Storage Virtual Machine

Details

Resource Allocation

Services

Name service switches are used to look up and retrieve user information to provide proper access to clients. The order of the services listed determines in which order the name service sources are consulted to retrieve information.

Name Service Switch

hosts:	files	dns	
namemap:	ldap	files	
group:	ldap	files	nis
netgroup:	ldap	files	nis
passwd:	ldap	files	nis

+ LDAP is the primary source of user information for name services and name mapping on this SVM.

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 (Configure NFS access to an existing 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:

Rule Index:

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:

	<input checked="" type="checkbox"/> Read-Only	<input checked="" type="checkbox"/> 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		

Superuser access is set to all

4. 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.