



Install and configure

NetApp NFS Plug-in for VMware VAAI

NetApp
June 11, 2024

Table of Contents

- Install and configure 1
 - Install NetApp NFS Plug-in for VMware VAAI 1
 - Configure export policies for ONTAP to allow VAAI over NFS 9

Install and configure

Install NetApp NFS Plug-in for VMware VAAI

Installing the NFS Plug-in involves enabling VMware vStorage for NFS on the NetApp storage system, verifying that VAAI (VMware vStorage APIs for Array Integration) is enabled on the VMware host, downloading and installing the plug-in on the VMware ESXi host, and verifying that the installation is successful.

Before you begin

- NFSv3 or NFSv4.1 must be enabled on the storage system.



NFSv4.1 is available only on ONTAP 9.0 systems and NFSv3 is available on both 7-Mode and Cluster-Mode systems.

- VMware vSphere 7.0U1 must be available.

For additional information about enabling NFS and using VMware vSphere, see the manuals listed in [Step 10](#).

About this task

- If you are using the VMware ESXi CLI to install the plug-in, start with [Step 1](#).
- If you are using Virtual Storage Console for VMware vSphere (VSC) to install the plug-in, start with [Step 3](#).

VSC enables VMware vStorage for NFS on the storage controller and enables VAAI on the ESXi host, which are steps [1](#) through [2](#) of this procedure.

- If you are using ONTAP tools for VMware vSphere to install the plug-in, start with [Step 3](#).

IP address conventions used:

- IP addresses of the form 192.168.42.2xx refer to ESXi server VMkernel ports.
- IP addresses of the form 192.168.42.6x refer to systems running Data ONTAP operating in 7-Mode.
- IP addresses of the form 192.168.42.8x refer to storage virtual machines (SVMs, formerly known as Vservers) on ONTAP systems.

Steps

1. Enable VMware vStorage for NFS:

If you use the...	Then...
ONTAP CLI	Enable VMware vStorage for NFS on the SVM: <code>vserver nfs modify -vserver vserver_name -vstorage enabled</code> <vserver_name> is the name of the SVM.
7-Mode CLI	Enable VMware vStorage for NFS on the storage system: <code>options nfs.vstorage.enable on</code>

If you use the...	Then...
7-Mode CLI for vFiler units	Enable the installation of NetApp NFS plug-in vStorage for NFS on the MultiStore vFiler unit hosting VMware NFS datastores: <code>vfiler run vfiler_name options nfs.vstorage.enable on</code>

2. Verify that VAAI is enabled on each ESXi host.

In VMware vSphere 5.0 and later, VAAI is enabled by default.

If you use the...	Then...
VMware ESXi CLI	<p>a. Verify that VAAI is enabled: <code>esxcfg-advcfg -g /DataMover/HardwareAcceleratedMove esxcfg-advcfg -g /DataMover/HardwareAcceleratedInit</code></p> <p>If VAAI is enabled, these commands display the following output:</p> <pre data-bbox="672 739 1487 1039">~ # esxcfg-advcfg -g /DataMover/HardwareAcceleratedMove Value of HardwareAcceleratedMove is **1** ~ # esxcfg-advcfg -g /DataMover/HardwareAcceleratedInit Value of HardwareAcceleratedInit is **1**</pre> <p>b. If VAAI is not enabled, enable VAAI: <code>esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedInit esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedMove</code></p> <p>These commands display the following output:</p> <pre data-bbox="672 1278 1487 1579">~ # esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedInit Value of HardwareAcceleratedInit is **1** ~ # esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedMove Value of HardwareAcceleratedMove is **1**</pre>

If you use the...	Then...
vSphere Client	<ol style="list-style-type: none"> a. Log in to the vCenter Server. b. For each ESXi server, click the server name. c. In the Software section of the Configuration tab, click Advanced Settings. d. Select DataMover, and then verify that the <code>DataMover.HardwareAcceleratedMove</code> and <code>DataMover.HardwareAcceleratedInit</code> parameters are set to 1.

3. Download the NetApp NFS Plug-in for VMware VAAI:
 - a. Go to the Download page at [NetApp NFS Plug-in for VMware VAAI downloads](#).
 - b. Download the latest software release for 2.0 and vSphere 7.0U1 and later.
4. Verify the binary with the signed image and the public key:
 - a. Download the following zip to the /tmp folder:

```
NetAppNasPlugin-<version>.Signed.zip
```

This zip contains the following files:

- NetAppNasPlugin-<version>.zip
- NetAppNasPlugin-<version>.zip.sig
- csc-prod-CFSG-NFS-Plugin.pem

- b. Obtain the public key from the certificate chain by using the following command:

```
openssl x509 -in csc-prod-CFSG-NFS-Plugin.pem -pubkey -noout > csc-prod-CFSG-NFS-Plugin.pub
```

- `csc-prod-CFSG-NFS-Plugin.pem` is the certificate chain present in `NetAppNasPlugin-<version>.Signed.zip`
- `csc-prod-CFSG-NFS-Plugin.pub` is a public key

- c. Verify the signed image with the public key:

```
openssl dgst -sha256 -verify csc-prod-CFSG-NFS-Plugin.pub -signature /tmp/NetAppNasPlugin-<version>.zip.sig /tmp/NetAppNasPlugin-<version>.zip
```

If verification is successful, the following output is displayed:

```
Verified OK
```

5. Install the plug-in on the ESXi host by running the following commands:

```
/etc/init.d/vaa-nasd stop
```

```
esxcli software component apply -d /tmp/<some_path>/NetAppNasPlugin-  
<version>.zip
```

```
/etc/init.d/vaai-nasd start
```

- <some_path> is the path to the location of the downloaded file
- NetAppNasPlugin-<version>.zip is contained in the downloaded zip

6. Verify that the plug-in was successfully installed on the host at the VMware ESXi command line:

```
esxcli software component list
```


The plug-in works automatically following the installation and reboot.

Using these commands ensures that the component remains compatible with the new vLCM feature of vSphere, available from 7.0x and later.

7. If you are installing the plug-in on a new host system, or the server running ONTAP has been newly configured, either create or modify export policy rules for the root volumes and for each NFS datastore volume on the ESXi servers that use VAAI at [Configure export policies for ONTAP to allow VAAI over NFS](#).

Skip this step if you are using Data ONTAP operating in 7-Mode.

You can use export policies to restrict access to volumes to specific clients. NFSv4 is required in the export policy for VAAI copy offloading to work, so you might need to modify the export policy rules for datastore volumes on SVMs. If you are using protocols other than NFS on a datastore, verify that setting NFS in the export rule does not remove those other protocols.

If you use...	Then...
ONTAP CLI	<p>Set <code>nfs</code> as the access protocol for each export policy rule for ESXi servers that use VAAI: <code>vserver export-policy rule modify -vserver vs1 -policyname mypolicy -ruleindex 1 -protocol nfs -rwrule krb5 krb5i any -rorule krb5 krb5i any</code></p> <p>In the following example:</p> <ul style="list-style-type: none"> • <code>vs1</code> is the name of the SVM. • <code>mypolicy</code> is the name of the export policy. • <code>1</code> is the index number of the rule. • <code>nfs</code> includes the NFSv3 and NFSv4 protocols. • The security style for RO (read-only) and RW (read-write) is either <code>krb5</code>, <code>krb5i</code>, or <code>any</code>. <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre>cluster1::> vserver export-policy rule modify -vserver vs1 -policyname mypolicy -ruleindex 1 -protocol nfs -rwrule krb5 krb5i any -rorule krb5 krb5i any</pre> </div>
ONTAP System Manager	<ol style="list-style-type: none"> From the Home tab, double-click the appropriate cluster. Expand the storage virtual machines (SVMs) hierarchy in the left navigation pane. <div style="margin-left: 20px;">  <p>If you are using a version of System Manager prior to 3.1, the term Vservers is used instead of Storage Virtual Machines in the hierarchy.</p> </div> In the navigation pane, select the storage virtual machine (SVM) with VAAI-enabled datastores, and then click Policies > Export Policies. In the Export Policies window, expand the export policy, and then select the rule index. <p>The user interface does not specify that the datastore is VAAI enabled.</p> Click Modify Rule to display the Modify Export Rule dialog box. Under Access Protocols, select NFS to enable all versions of NFS. Click OK.

8. If you are using Data ONTAP operating in 7-Mode, execute the `exportfs` command for exporting volume paths.

Skip this step if you are using ONTAP.

For more information about the `exportfs` command, see the [Data ONTAP 8.2 File Access and Protocols Management Guide for 7-Mode](#).

When exporting the volume, you can specify a host name or IP address, a subnet, or a netgroup. You can specify IP address, subnet, or hosts for both the `rw` and `root` options. For example:

```
sys1> exportfs -p root=192.168.42.227 /vol/VAAI
```

You also can have a list, separated by colons. For example:

```
sys1> exportfs -p root=192.168.42.227:192.168.42.228 /vol/VAAI
```

If you export the volume with the `actual` flag, the export path should have a single component for copy offload to work properly. For example:

```
sys1> exportfs -p actual=/vol/VAAI,root=192.168.42.227 /VAAI-ALIAS
```



Copy offload does not work for multicomponent export paths.

9. Mount the NFSv3 or NFSv4.1 datastore on the ESXi host:

- a. To mount the NFSv3 datastore, execute the following command:

```
esxcli storage nfs add -H 192.168.42.80 -s share_name -v volume_name
```

To mount the NFSv4.1 datastore, execute the following command:

```
esxcli storage nfs41 add -H 192.168.42.80 -s share_name -v volume_name -a AUTH_SYS/SEC_KRB5/SEC_KRB5I
```

The following example shows the command to be run on ONTAP for mounting the datastore and the resulting output:

```
~ # esxcfg-nas -a onc_src -o 192.168.42.80 -s /onc_src
Connecting to NAS volume: onc_src
/onc_src created and connected.
```

For systems running Data ONTAP operating in 7-Mode, the `/vol` prefix precedes the NFS volume name. The following example shows the 7-Mode command for mounting the datastore and the resulting output:


```

~ # esxcfg-nas -a vms_7m -o 192.168.42.69 -s /vol/vms_7m
Connecting to NAS volume: /vol/vms_7m
/vol/vms_7m created and connected.

```

b. To manage NAS mounts:

```
esxcfg-nas -l
```

The following output is displayed:

```

VMS_vol103 is /VMS_vol103 from 192.168.42.81 mounted available
VMS_vol104 is VMS_vol104 from 192.168.42.82 mounted available
dbench1 is /dbench1 from 192.168.42.83 mounted available
dbench2 is /dbench2 from 192.168.42.84 mounted available
onc_src is /onc_src from 192.168.42.80 mounted available

```

Upon completion, the volume is mounted and available in the /vmfs/volumes directory.

10. Verify that the mounted datastore supports VAAI by using one of the following methods:

If you use...	Then...
ESXi CLI	<pre> vmkfstools -Ph /vmfs/volumes/onc_src/ The following output is displayed: NFS-1.00 file system spanning 1 partitions. File system label (if any): onc_src Mode: public Capacity 760 MB, 36.0 MB available, file block size 4 KB UUID: fb9cccc8-320a99a6-0000-000000000000 Partitions spanned (on "notDCS"): nfs:onc_src NAS VAAI Supported: YES Is Native Snapshot Capable: YES ~ # </pre>
vSphere Client	<ol style="list-style-type: none"> Click ESXi Server > Configuration > Storage. View the Hardware Acceleration column for an NFS datastore with VAAI enabled.

For more information about VMware vStorage over NFS, see the following:

[ONTAP 9 NFS reference overview](#)

[Data ONTAP 8.2 File Access and Protocols Management Guide for 7-Mode](#)

For details about configuring volumes and space in the volumes, see the following:

[Logical storage management overview with the CLI](#)

[Data ONTAP 8.2 Storage Management Guide For 7-Mode](#)

For more information about the VMware vSphere Lifecycle Manager, which can also be used to install and manage plugins on multiple hosts using the vCenter web client GUI, see the following:

[About VMware vSphere Lifecycle Manager](#)

For information about using VSC to provision NFS datastores and create clones of virtual machines in the VMware environment, see the following:

[Virtual Storage Console 6.2.1 for VMware vSphere Installation and Administration Guide](#)

For more information about using ONTAP tools for VMware vSphere to provision NFS datastores and create clones of virtual machines in the VMware environment, see the following:

[ONTAP tools for VMware vSphere Documentation](#)

For more information about working with NFS datastores and performing cloning operations, see the following:

[VMware vSphere Storage](#)

11. If you are using Data ONTAP operating in 7-Mode, execute the `sis on` command to enable the datastore volume for copy offloading and deduplication.

For ONTAP, view the efficiency details for a volume:

```
volume efficiency show -vserver vservice_name -volume volume_name
```



For AFF (AFF) systems, volume efficiency is enabled by default.

If the command output does not display any volumes with storage efficiency enabled, then enable efficiency:

```
volume efficiency on -vserver vservice_name -volume volume_name
```

Skip this step if you are using VSC or ONTAP tools for VMware vSphere to set up the volumes because volume efficiency is enabled on the datastores by default.

```

sys1> volume efficiency show
This table is currently empty.

sys1> volume efficiency on -volume testvoll
Efficiency for volume "testvoll" of Vserver "vs1" is enabled.

sys1> volume efficiency show
Vserver      Volume          State    Status    Progress
Policy
-----
vs1          testvoll       Enabled  Idle      Idle for 00:00:06 -

```

For details about enabling deduplication on the datastore volumes, see the following:

[Logical storage management overview with the CLI](#)

[Data ONTAP 8.2 File Access and Protocols Management Guide for 7-Mode](#)

After you finish

Use the NFS plug-in space reservation and copy offload features to make routine tasks more efficient:

- Create virtual machines in the thick virtual machine disk (VMDK) format on NetApp traditional volumes or FlexVol volumes, and reserve space for the file when you create it.
- Clone existing virtual machines within or across NetApp volumes:
 - Datastores that are volumes on the same SVM on the same node.
 - Datastores that are volumes on the same SVM on different nodes.
 - Datastores that are volumes on the same 7-Mode system or vFiler unit.
- Perform cloning operations that finish faster than non-VAAI clone operations because they do not need to go through the ESXi host.

Configure export policies for ONTAP to allow VAAI over NFS

You must configure export policies to provide compliance between VMware vStorage APIs for Array Integration (VAAI) storage features over the NFS server and NetApp storage. In ONTAP, volume exports are restricted by export policies that are applied on storage virtual machines (SVMs, formerly known as Vservers).

Before you begin

- NFSv4 calls must be allowed by the relevant NFS volumes.
- The root user must be retained as the primary user.
- NFSv4 must be allowed on all of the interconnected parent volumes.
- The option for VAAI support must be set on the relevant NFS server.

About this task

You can configure different export policies for multiple conditions and protocols.

Steps

1. If an export policy is not created, then create an export policy for the SVM in the root volume of the VMware ESXi host that contains the SVM name, policy name, default rule index, protocol, and so on:

```
vserver export-policy rule modify -vserver vserver name -policyname default
-ruleindex rule index -protocol NFSv3\|NFSv4
```

2. Modify the export policy to allow both NFSv3 and NFSv4 protocols with the following conditions:

- You must have configured the export policy rule for the respective ESX server and the volume with all of the relevant access permissions.
- You must have set the values of RW, RO, and Superuser to `SYS` or `ANY` for the client match.
- You must have allowed the NFSv3 and NFSv4 protocol.

The Access Protocol in the export policy is set as follows:

- Access Protocol = `nfs` (to include all versions of NFS)
- Access Protocol = `nfsv3,nfsv4` (NFSv3 for NFSv3 datastore access) and `NFSv4` (NFSv4 for NFSv4.1 datastore access)).

The following commands display the SVM details and set the export policy:

```
cm3240c-rtp::> vol show -vserver vmware -volume vmware_VAAI
-fields policy (volume
show)
vserver volume          policy                  junction-path
-----
vmware  vmware_VAAI  vmware_access  /VAAI
```

```
cm3240c-rtp::> export-policy rule show -vserver vmware -policyname
vmware_access-ruleindex 2(vserver export-policy rule show)
```

```
Vserver: vmware
Policy Name: vmware_access
Rule Index: 1
Access Protocol: nfs3,nfs4 (can also be nfs for NFSv3)
Client Match Spec: 192.168.1.6
RO Access Rule: sys
RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
Superuser Security Flavors: sys
Honor SetUID Bits In SETATTR: true
Allow Creation of Devices: true
```

Any policy change is applied to all of the volumes using the relevant policy and is not restricted to the NFS datastore volumes.

3. Modify the export policy to set the Superuser as SYS with the following conditions:

- You must have configured all of the parent volumes in the junction path with read access permission to the root volume, NFSv4 access, and VAAI access to the junction volume.

The Superuser of the root volume for the SVM is set to SYS for the relevant client.

- You must have denied write access permission for the SVM root volume. The following commands display the SVM details and set the export policy:

```
cm3240c-rtp::> vol show -vserver vmware -volume vmware_root -fields
policy,
junction-path (volume show)
vserver volume policy junction-path
-----
vmware vmware_root root_policy /
```

```
cm3240c-rtp::> export-policy rule show -vserver vmware -policyname
root_policy
-ruleindex 1 (vserver export-policy rule show)

Vserver: vmware
Policy Name: root_policy
Rule Index: 1
Access Protocol: nfs <--- as in scenario 1, set to nfs or nfs3,nfs4
Client Match Spec: 192.168.1.5
RO Access Rule: sys
RW Access Rule: never <--- this can be never for security reasons
User ID To Which Anonymous Users Are Mapped: 65534
Superuser Security Flavors: sys <--- this is required for VAAI to
be set, even
in the parent volumes like vsroot
Honor SetUID Bits In SETATTR: true
Allow Creation of Devices: true
```

The root user is retained because the Superuser is set to SYS. Therefore, the root user can access the volume that has the junction path /VAAI.

If additional volumes exist in the junctions between the root volume and the vmware_VAAI volume, then those volumes should have a policy rule for the respective client, where the Superuser is set to SYS or ANY.

In most cases, the root volume uses a policy with the Policy Name set to default.

Any policy change is applied to all of the volumes using the relevant policy and is not restricted to the

root volume.

4. Enable the vStorage feature: `nfs modify -vserver vserver_name vmware -vstorage enabled`

The NFS service on the SVM requires enabling the vStorage feature.

5. Verify that the vStorage feature is enabled:

```
nfs show -fields vstorage
```

The output should display enabled:

```
cm3240c-rtp::> nfs show -fields vstorage
vserver vstorage
-----
vmware  enabled
```

6. Create the export policy:

```
vserver export-policy rule create
```

The following commands create the export policy rule:

```
User1-vserver2::> protocol export-policy rule create -vserver vs1
-policyname default -clientmatch 0.0.0.0/0 -rorule any -rwrule any
-superuser
any -anon 0

User1-vserver2::> export-policy rule show vserver export-policy rule
show)
Virtual      Policy      Rule      Access   Client      RO
Server       Name        Index     Protocol Match      Rule
-----
-----
vs1          default     1         any      0.0.0.0/0   any

User1-vserver2::>
```

7. Display the export policy:

```
vserver export-policy show
```

The following commands display the export policy:

```
User1-vserver2::> export-policy show (vserver export-policy show)
```

```
Virtual Server    Policy Name
```

```
-----
```

```
vs1                default
```

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.